(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2002－521962
（P2002－521962A）
(43)公表日　平成14年７月16日(2002.7.16)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｋ　17/00	Ｔ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｈ０４Ｌ　12/22		５Ｊ１０４
Ｈ０４Ｌ　9/32		9/00	６０１Ｃ	５Ｋ０３０
12/22			６７５Ａ	

審査請求　未請求　予備審査請求　有　（全 53 頁）

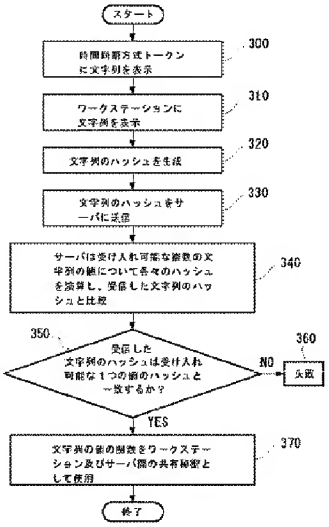
(21)出願番号　特願2000－563030(P2000－563030)
(86)（22)出願日　平成11年７月30日(1999.7.30)
(85)翻訳文提出日　平成13年１月31日(2001.1.31)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／１７２３２
(87)国際公開番号　ＷＯ００／０７３２６
(87)国際公開日　平成12年２月10日(2000.2.10)
(31)優先権主張番号　０９／１２６，６５９
(32)優先日　平成10年７月31日(1998.7.31)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　サンマイクロシステムズ　インコーポレーテッド
アメリカ合衆国、94043　カリフォルニア州、マウンテン　ビュー、ガルシア　アヴェニュー　2550
(72)発明者　バールマン　ラディア　ジェイ
アメリカ合衆国、01720　マサチューセッツ州、アクトン、ハックルベリー　レイン　10
(74)代理人　弁理士　上野　登

最終頁に続く

(54)【発明の名称】　認証トークンを使用して共有秘密を確立する方法及びシステム

(57)【要約】
認証トークンを用いて複数の装置間に共有秘密を確立する方法及びシステム。認証トークンはローカルデバイス及びリモートデバイス間に共有秘密を確立するために用いられ、ユーザ認証、データ暗号化、及びデータ完全性の保護を実現する。認証トークンは様々の方法で用いられ、ユーザを認証する。まず、時間同期方式の認証トークンが第一文字列を生成し、ワークステーションに伝達する（３１０）。ワークステーションは第一文字列を操作して第二文字列を生成し（３２０）、第二文字列をサーバに送信する（３３０）。次に、サーバは第二文字列を一致する可能性のある複数の文字列の値と比較し、第一文字列を特定する（３４０）。また、別の実施例としては、サーバからのチャレンジがチャレンジ＆レスポンス方式の認証トークンにより受信及び処理され、文字列を生成する方法もある。その後、生成された文字列はワークステーションに伝達されて共有秘密を確立する（３７０）。また、類似の技術を用い、スマートカードを使用してローカルデバイス及びリモートデバイス間に共有秘密を確立することも可能である。



【特許請求の範囲】
【請求項１】　複数の装置間に共有秘密を確立する方法であって、該方法は、
認証トークンを提供する工程と、
前記認証トークンで第一文字列を生成する工程と、
前記第一文字列をローカルデバイスに伝達する工程（３１０）と、
前記ローカルデバイスで前記第一文字列から第二文字列を作成する工程（３２０）と、
前記第二文字列をリモートデバイスに送信する工程（３３０）と、
予測された複数の文字列の値から前記第二文字列を一義化する工程（３４０）と、
予測された複数の文字列の値から最低１つを利用して、前記ローカルデバイス及び前記リモートデバイス間に共有秘密を確立する工程（３７０）と、
から構成される。
【請求項２】　請求項１の方法であって、更に、
前記リモートデバイスとの間に共有秘密を確立するために、前記第一文字列を用いて共有秘密鍵交換プロトコルを実行する工程から構成される。
【請求項３】　請求項２の方法において、
前記実行の工程は、
予測された複数の文字列の値から前記第一文字列を一義化する工程と、
前記第一文字列が一義化された後で、前記共有秘密鍵交換プロトコルを実行する工程と、
を含む。
【請求項４】　請求項２の方法において、
前記実行の工程は、
予測された複数の文字列の値から前記第一文字列を一義化する工程と、
前記第一文字列が一義化される間に、前記共有秘密鍵交換プロトコルを実行する工程と、
を含む。

【請求項５】　請求項２の方法において、
　前記実行の工程は、
　前記共有秘密鍵交換プロトコルを実行する工程と、
　前記共有秘密鍵交換プロトコルが実行された後で、予測された複数の文字列の値から前記第一文字列を一義化する工程と、
　を含む。
【請求項６】　請求項２の方法において、
　前記実行の工程は、前記リモートデバイスとの間で共有秘密を確立するために、前記第一文字列と個人識別番号を用いて共有秘密鍵交換プロトコルを実行する工程を含む。
【請求項７】　請求項１の方法において、
　前記作成の工程は、前記第一文字列の関数を実行し、前記第二文字列を生成する工程を含む。
【請求項８】　請求項１の方法において、
　前記提供の工程は、スマートカードを提供する工程を含む。
【請求項９】　請求項１の方法は、更に、
　前記ローカルデバイスが前記共有秘密を有することを前記リモートデバイスに証明する工程から構成される。
【請求項１０】　請求項９の方法において、
前記証明の工程は、
　第三文字列を前記リモートデバイスから前記ローカルデバイスに伝達する工程と、
　前記共有秘密及び前記第三文字列のうち少なくともいずれか１つを用いて、前記ローカルデバイスで関数を実行し、出力データを生成する工程と、
　前記出力データを前記リモートデバイスに送信する工程と、
　前記出力データを予測された文字列の値と比較し、前記ローカルデバイスが前記共有秘密を有することを証明する工程と、
　を含む。
【請求項１１】　請求項１の方法は、更に、

前記リモートデバイスが前記共有秘密を有することを前記ローカルデバイスに証明する工程から構成される。

【請求項１２】　請求項１１の方法において、

前記証明の工程は、

前記ローカルデバイスから前記リモートデバイスに第三文字列を伝達する工程と、

前記共有秘密及び前記第三文字列のうち少なくともいずれか１つを用いて、前記リモートデバイスで関数を実行し、出力データを生成する工程と、

前記出力データを前記ローカルデバイスに送信する工程と、

前記出力データを予測された文字列の値と比較し、前記リモートデバイスが前記共有秘密を有することを証明する工程と、

を含む。

【請求項１３】　請求項１の方法において、

前記作成の工程は、前記第一文字列と個人識別番号を用いて前記第二文字列を作成する工程を含む。

【請求項１４】　請求項１の方法において、

前記作成の工程は、ハッシュ関数を実行して前記第一文字列から前記第二文字列を作成する工程を含む。

【請求項１５】　請求項１の方法において、

前記送信の工程は、前記第二文字列の一部分のみを前記リモートデバイスに送信する工程を含む。

【請求項１６】　請求項１の方法は、更に、

予測された複数の文字列の値のうち少なくともいずれか１つから前記第二文字列を一義化するために必要な情報を求める命令を、前記リモートデバイスから前記ローカルデバイスに伝達する工程から構成される。

【請求項１７】　請求項１６の方法は、更に、

予測された複数の文字列の値のうち少なくともいずれか１つから前記第二文字列を一義化するよう求める前記命令に従って、ワークステーションで出力値を生成する工程から構成される。

【請求項１８】　請求項１の方法は、更に、
　起動コードにより前記認証トークンを起動する工程から構成される。
【請求項１９】　請求項１の方法において、
　前記提供の工程は、少なくとも複数の装置のいずれか１つに対し、ほぼ時間同期方式の認証トークンを提供する工程から構成される。
【請求項２０】　複数の装置間に共有秘密を確立する方法であって、該方法は、
　認証トークンを提供する工程と、
　リモートデバイスから前記認証トークンに第一文字列を伝達する工程と、
　前記認証トークンを用いて前記第一文字列を処理し、第二文字列を生成する工程と、
　前記第二文字列をローカルデバイスに送信する工程と、
　前記第二文字列を利用してリモートデバイスとの間に共有秘密を確立する工程と、
　から構成される。
【請求項２１】　請求項２０の方法は、更に、
　起動コードにより前記認証トークンを起動する工程から構成される。
【請求項２２】　請求項２０の方法において、
前記送信の工程は、前記第二文字列と併せて個人識別番号を前記ローカルデバイスに伝達する工程を含む。
【請求項２３】　請求項２０の方法において、
　前記利用の工程は、共有秘密を確立するために、前記第二文字列に対して共有秘密鍵交換プロトコルを実行する工程を含む。
【請求項２４】　請求項２０の方法において、
　前記利用の工程は、共有秘密を確立するために、前記第二文字列及び前記個人識別番号に対して前記共有秘密鍵交換プロトコルを実行する工程を含む。
【請求項２５】　複数の装置間に共有秘密を確立する方法であって、該方法は、
　認証トークンを提供する工程と、
　前記認証トークンを利用して複数の装置間に共有秘密を確立する工程と、
から構成される。

【請求項２６】　請求項２５の方法において、
前記提供の工程は、スマートカードを提供する工程を含む。
【請求項２７】　複数の装置間に共有秘密を確立するシステムであって、該システムは、
　認証トークンと、
　ローカルデバイスと、
　リモートデバイスと、
　から構成され、前記システムにおいては、
　前記認証トークンを使用し、前記ローカルデバイス及び前記リモートデバイス間に共有秘密を確立する。
【請求項２８】　請求項２７のシステムにおいて、
　前記認証トークンは前記リモートデバイスとほぼ時間同期されている。
【請求項２９】　請求項２７のシステムにおいて、
　前記認証トークンはプロセッサを備える。
【請求項３０】　請求項２７のシステムにおいて、
　前記認証トークンは入力データを受け取るよう構成されている。
【請求項３１】　請求項２７のシステムにおいて、
前記認証トークンは出力データを生成するよう構成されている。
【請求項３２】　請求項２７のシステムにおいて、
前記認証トークンはディスプレーを備える。
【請求項３３】　請求項３２のシステムにおいて、
　前記認証トークンは前記ディスプレーに表示可能な文字列を生成する手段を備える。
【請求項３４】　請求項２７のシステムにおいて、
　前記ローカルデバイスはワークステーションである。
【請求項３５】　請求項２７のシステムにおいて、
　前記リモートデバイスはサーバである。
【請求項３６】　請求項２７のシステムにおいて、
　前記認証トークンはスマートカードである。

【請求項３７】　複数の装置間に共有秘密を確立するシステムであって、該システムは、
　ローカルデバイスと、
　リモートデバイスと、
　認証トークンと、
　前記認証トークンで第一文字列を生成する手段と、
　前記第一文字列を前記ローカルデバイスに伝達する手段と、
　所定の関数を用いて前記第一文字列を操作し、第二文字列を生成する手段と、
　前記第二文字列を前記リモートデバイスに送信する手段と、
　予測された複数の文字列の値のうち少なくともいずれか１つと前記第二文字列を照合し、前記ローカルデバイス及び前記リモートデバイス間に共有秘密を確立する手段と、
から構成される。
【請求項３８】　請求項３７のシステムにおいて、
　前記認証トークンは、ほぼ時間同期されたトークンである。
【請求項３９】　請求３７のシステムにおいて、
　前記操作の手段は、前記第一文字列を入力データとして用いてハッシュ関数を実行し、前記第二文字列を生成する手段を含む。
【請求項４０】　請求項３７のシステムにおいて、
　前記操作の手段は、前記第一文字列及び個人識別番号を入力データとして用いてハッシュ関数を実行し、前記第二文字列を生成する手段を含む。
【請求項４１】　請求項３７のシステムは、更に、
　前記第一文字列を用いて共有秘密鍵交換プロトコルを実行し、共有秘密を生成する手段を備える。
【請求項４２】　請求項４１のシステムにおいて、
　前記実行の手段は、前記第一文字列と個人識別番号を用いて共有秘密鍵交換プロトコルを実行し、共有秘密を生成する手段を備える。
【請求項４３】　請求項３７のシステムにおいて、
　前記送信の手段は、前記第二文字列のビットの総数に満たないビットを前記リ

モートデバイスに送信する手段を含む。
【請求項４４】　請求項３７のシステムは、更に、
　予測された複数の文字列の値のうち少なくともいずれか１つから前記第二文字列を一義化するのに必要な情報を求める命令を、前記リモートデバイスから前記ローカルデバイスに転送する手段を備える。
【請求項４５】　請求項４４のシステムにおいて、
前記転送の手段は、前記リモートデバイスから前記ローカルデバイスに転送される前記命令を定数に与え、ハッシュアルゴリズムを用いて前記第二文字列と共に処理する手段を備える。
【請求項４６】　請求項３７のシステムにおいて、
　前記生成の手段は、起動コードにより前記認証トークンを起動する手段を備える。
【請求項４７】　複数の装置間に共有秘密を確立するシステムであって、該システムは、
　ローカルデバイスと、
　リモートデバイスと、
　認証トークンと、
　前記リモートデバイスを用いて第一文字列を特定する手段と、
　前記第一文字列を前記認証トークンに送信する手段と、
　前記第一文字列を処理し、第二文字列を生成する手段と、
　前記第二文字列を前記ローカルデバイスに伝達し、前記リモートデバイス及び前記ローカルデバイスが前記第二文字列を秘密として共有するようにした手段と、
から構成される。
【請求項４８】　請求項４７のシステムにおいて、
　前記認証トークンは、チャレンジ＆レスポンス方式トークンである。
【請求項４９】　請求項４７のシステムは、更に、
　前記認証トークンに起動コードを入力する手段を備える。
【請求項５０】　請求項４７のシステムは、更に、

前記ローカルデバイスに個人識別番号を入力する手段を備える。

【請求項５１】　請求項４７のシステムは、更に、

前記第二文字列を用いて共有秘密鍵交換プロトコルを実行する手段を備える。

【請求項５２】　複数の装置間に共有秘密を確立する方法であって、該方法は、

スマートカードを提供する工程と、

前記スマートカードからローカルデバイスにデータ通信を行う工程と、

前記データを利用して前記ローカルデバイス及びリモートデバイス間に共有秘密を確立する工程と、

から構成される。

【請求項５３】　請求項５２の方法は、更に、

起動コードにより前記スマートカードを起動する工程を含む。

【請求項５４】　請求項５３の方法において、

前記起動コードは個人識別番号である。

【請求項５５】　請求項５３の方法において、

前記起動コードはバイオメトリクスである。

【請求項５６】　請求項５２の方法において、

前記提供の工程は、内部クロックを備えたスマートカードを提供する工程を含む。

【請求項５７】　請求項５２の方法において、

前記提供の工程は、外部クロックを利用したスマートカードを提供する工程を含む。

【請求項５８】　複数の装置間に共有秘密を確立する方法であって、該方法は、

スマートカードを提供する工程と、

前記スマートカード及びリモートデバイス間に共有秘密を確立する工程と、

前記スマートカードからローカルデバイスに前記共有秘密を伝達し、前記ローカルデバイス、前記スマートカード、及び前記リモートデバイス間に前記共有秘密を確立する工程と、

から構成される。
【請求項５９】　請求項５８の方法において、
前記確立の工程は、
前記スマートカードで第一文字列を生成する工程と、
前記第一文字列を前記リモートデバイスに伝達する工程と、
前記第一文字列を利用して前記リモートデバイスとの間に共有秘密を確立する工程と、
を含む。
【請求項６０】　請求項５８の方法において、
前記確立の工程は、
前記リモートデバイスから前記スマートカードに第一文字列を伝達する工程と、
前記スマートカードにおいて前記第一文字列を処理し、第二文字列を生成して共有秘密を確立する工程と、
を含む。
【請求項６１】　請求項５８の方法は、更に、
起動コードにより前記スマートカードを起動する工程を含む。
【請求項６２】　請求項６１の方法において、
前記起動コードは個人識別番号である。
【請求項６３】　請求項６１の方法において、
前記起動コードはバイオメトリクスである。
【請求項６４】　請求項５８の方法において、
前記提供の工程は、内部クロックを備えたスマートカードを提供する工程を含む。
【請求項６５】　請求項５８の方法において、
前記提供の工程は、外部クロックを利用するスマートカードを提供する工程を含む。
【請求項６６】　複数の装置間に共有秘密を確立する方法であって、該方法は、

スマートカードを提供する工程と、
前記スマートカード及びリモートデバイス間に共有秘密を確立する工程と、
前記リモートデバイス及びローカルデバイス間のトランザンクションにおいて、前記スマートカード及び前記共有秘密を利用する工程と、
から構成される。
【請求項６７】　請求項６６の方法において、
前記確立の工程は、
前記スマートカードで第一文字列を生成する工程と、
前記第一文字列を前記リモートデバイスに伝達する工程と、
前記第一文字列を利用して前記リモートデバイスとの間に共有秘密を確立する工程と、
を含む。
【請求項６８】　請求項６６の方法において、
前記確立の工程は、
前記リモートデバイスから前記スマートカードに第一文字列を伝達する工程と、
前記スマートカードにおいて前記第一文字列を処理し、第二文字列を生成して共有秘密を確立する工程と、
を含む。
【請求項６９】　請求項６６の方法は、更に、
起動コードにより前記スマートカードを起動する工程を含む。
【請求項７０】　請求項６９の方法において、
前記起動コードは個人識別番号である。
【請求項７１】　請求項６９の方法において、
前記起動コードはバイオメトリクスである。
【請求項７２】　請求項６６の方法において、
前記提供の工程は、内部クロックを備えたスマートカードを提供する工程を含む。
【請求項７３】　請求項６６の方法において、

前記提供の工程は、外部クロックを利用するスマートカードを提供する工程を含む。

【発明の詳細な説明】

【０００１】

（発明の技術分野）

本発明は、概して、通信の安全保護に関し、更に詳しくは、通信媒体を介して接続された装置間に認証トークンを用いて共有秘密を確立し、ユーザ認証、データ暗号化、及びデータ完全性の保護を実現するための方法及びシステムに関する。

【０００２】

（発明の背景技術）

従来から、ネットワークユーザはユーザ名とパスワードを入力するだけでネットワーク資源やネットワークの他のユーザにアクセスすることができる。ユーザ名とパスワードの入力によってネットワークにアクセスした後、ユーザは通常、ネットワークに接続している間、暗号化されていないデータを保護手段のないまま送受信する。つまり、機密保護を欠いたまま、データは「ありのまま」の状態で通信回線を介して送信される。このような従来のネットワークへのアクセス方法及びネットワークを介した通信方法では、ネットワークの完全性に関して多くの問題が発生する。

【０００３】

第一に、ユーザ名とパスワードのみでは、ネットワークへのアクセスに対して最低限のユーザ認証しか得ることができない。パスワードが単純な（たとえばユーザの誕生日である）場合、ハッカーは容易にユーザのパスワードを特定し、ユーザ名を詐称する情報によりネットワークにアクセスしてしまう。第二に、ネットワーク上での非暗号化データの送受信は、盗聴される危険性が高い。ネットワーク通信回線を介して送信されるデータが盗聴され、ユーザのネットワークセッションを乗っ取るなどの不正な目的のために、盗聴したデータが悪用される恐れがある。また、非暗号化データは、データを改変（たとえばビットを削除または変更）したり、隠れた周辺装置にデータをコピー（ユーザの感知しない遠隔記憶装置にデータをコピー）したりすることのできる悪質なソフトウェアによる被害を受けやすい。

【０００４】
現在、「持っているもの」（パスワードのように「知っているもの」とは全く異なる）に基づいた別レベルのユーザ認証を実現するために、認証トークンに頼るユーザが多い。認証トークンは、単に記憶されるパスワードとは異なり、持ち運ぶことのできる物理的な装置である。現在では、様々の認証トークンが市販されている。これらの認証トークンには、時間同期方式の認証トークン、チャレンジ＆レスポンス方式の認証トークン、及びスマートカードが挙げられる。
【０００５】
時間同期方式の認証トークンは、通常、様々の異なる文字列（パスワード等）をほぼ一定の間隔ごとに（たとえば毎分）表示するものである。この場合、たとえばサーバとトークンが分単位の時刻を用いて（所定の許容可能な誤差の範囲内で）同期をとり、文字列（たとえば、トークンとサーバのみが把握する秘密コードにより分単位の時刻を暗号化したもの）を生成する。次に、ユーザがトークンに表示された文字列をワークステーションに入力すると、サーバに対してユーザ認証が行われる。ワークステーションは文字列を暗号化されない状態でサーバに送信する。サーバは文字列を一覧と照合し、文字列が直前の数分前（タイピングや転送による遅延を許容するため）にトークンにより生成されたか否かを判定する。
【０００６】
チャレンジ＆レスポンス方式トークンは、カードなどのキーパッドを備えた装置である。従来、このトークンを使う認証の際は、たとえば、最初にユーザがサーバに接触すると、サーバはチャレンジ（たとえば文字列）を生成し、そのチャレンジをローカルコンピュータを介してユーザに送信する。次に、ユーザがトークンにチャレンジを入力すると、トークンはチャレンジを処理し、レスポンス（たとえば別の文字列）を表示する。ユーザがレスポンスをサーバに送信すると、サーバはレスポンスを所定の文字列の値と照合する。一致するものがある場合は、サーバは要求されたアクセスを許可する。
【０００７】
スマートカードは、中央演算装置（CPU）とメモリを備えた装置である。スマ

ートカードは、スマートカードリーダーの近くに挿入または配置されると、リーダーと交信してデータを転送するか、または所望の機能を実行する。スマートカードはあらゆる形状をとる。たとえば、クレジットカードや、衣類の一部分に付けるペンダントの形をとる場合もある。

【０００８】

上述した認証トークンは、いずれも操作用の認証コードを必要とする。起動コードは個人識別番号（ＰＩＮ）またはバイオメトリクスの形態をとる。たとえば、時間同期方式の認証トークンを操作するには、ユーザは文字列を入力するか、またはトークンの一部分に親指を接触させるよう求められる。チャレンジ＆レスポンス方式のトークンでは、起動コードを用いてトークンを起動してからチャレンジを入力するよう求められる。最後に、ある種のスマートカードは、スマートカードに記憶された情報（たとえば文字列）に対して「ロックの解除」を行うために、ユーザに起動コードを入力するよう要求する。通常、誤ったコードを何回か入力すると、スマートカードは「ロック」された状態となり、記憶された情報へのアクセスを拒否する。情報がアクセス可能な場合は、スマートカードリーダーは情報をワークステーションに伝達し、その情報を用いて認証を行う。

【０００９】

通常、時間同期方式の認証トークン、チャレンジ＆レスポンス方式の認証トークン、及びスマートカードを用いる場合、それらの中で生成される文字列の値は、ユーザのワークステーション及びリモートコンピュータ間で、暗号化されない状態のまま転送される。その結果、ユーザ及びリモート端末間における通信は全て、乗っ取り犯や盗聴者による危害、つまり未保護コードの解読や通信情報の盗聴などが容易に行われる危険にさらされる。

【００１０】

従来、認証トークンの使用はユーザ認証のみを目的としている。セッション鍵、つまりセッション中に情報を暗号化または解読するのに使用する量が全く確定されないため、セッションの完全性や機密性は一切保証されない。更に、クライアントが正当なサーバと交信しているか否かをクライアント自身が知る手立ても全くない。認証トークンにより生成される文字列の値は、通常、３２ビット未満

の重要な情報を含む。これにより、表示に要するコストが抑制できると共に、ユーザに長い文字列を入力するよう要求するのを回避することが可能であるが、それとひきかえに、システムは様々の攻撃に対して脆弱なものとなってしまう。

【００１１】

共有秘密鍵交換プロトコルを用いれば、共有秘密を有する２台のコンピュータにおいて共有秘密に攻撃を受ける危険を冒すことなく、より強力な共有秘密を確立することができる。更に、より強力な共有秘密は、コンピュータ間で交換されるデータの暗号化に用いられる。これらのプロトコルは市販されており、「ベロヴィン・メリット共有秘密鍵交換プロトコル」（Bellovin-Merritt shared secret exchange protocol）や「強力パスワード限定認証鍵交換」（SPEKE—Strong Password only Authentication Key Exchange）などがある。共有秘密鍵交換プロトコルのいくつかは、『ネットワークセキュリティ—公共の世界における通信の機密』（カウフマン（Kaufman）、パールマン（Perlman）、スペシナー（Speciner）共著、出版：プレンティスホール・ピーティーアール（Prentice Hall PTR）、発行：1995年）（以下、『ネットワークセキュリティ』）に説明されている。ベロヴィン・メリット共有秘密交換プロトコルについての論議は、『ネットワークセキュリティ』の第249～253頁、及び米国特許No.5241599に記載されている。SPEKEについての論議は、『コンピュータ通信レビュー（Computer Communication Review）』第26巻（1996年10月発行、エーシーエム・シグコム（ACM SIGCOMM）刊）の第5番、第5～26頁、Ｄ.ジャブロン氏による「強力パスワード限定認証鍵交換（Strong Password only Authentication Key Exchange）」に掲載されている。共有秘密鍵交換プロトコルは、暗号化されていないパスワードの送信を回避することにより、パスワードをベースとしたシステムを強化する。共有秘密鍵交換プロトコルを認証トークンと併用するとセッションの安全性を強化することができるが、現状では併用されていない。従って、認証トークンと共有秘密鍵交換プロトコルの両方を用いることにより、適切なユーザ認証、データ暗号化、及びデータ完全性の保護を実現するための解決方法が求められている。

【００１２】

（発明の開示）

上記の問題点に基づき、ネットワークを介して交信する当事者間に認証トークンを用いて共有秘密を確立し、適切なユーザ認証、データ暗号化、及びデータ完全性の保護を実現するのが望ましい。

【００１３】

本発明に係る方法及び装置は、上記の要求を満たしている。具体的には、複数の装置間に共有秘密を確立する方法は、認証トークンを提供する工程と、認証トークンを利用して複数の装置間に共有秘密を確立する工程から構成される。

【００１４】

共有秘密を複数の装置間に確立するシステムは、認証トークン、ローカルデバイス及びリモートデバイスを備え、このシステムにおいては、認証トークンを用いてローカルデバイス及びリモートデバイス間に共有秘密が確立される。

【００１５】

本発明のその他の要求、特徴、及び利点は、以下に示した説明から明らかであり、発明の実施により理解されるであろう。上記の概説及び以下の詳説は例示と解説のためであり、特許請求される本発明を詳述するものである。

【００１６】

（発明の最良の実施形態）

本明細書の一部を成す添付図面は、本発明の実施形態を図示し、本発明の概説及び詳説と共に本発明の原理を説明するものである。

【００１７】

以下、添付図面に示す本発明の実施形態の構成及び動作について詳細に説明する。尚、図面及び下記の説明において、類似の要素及び動作については同一の符号を用いて参照した。

【００１８】

本発明に係る方法及び装置によれば、ネットワーク上で交信する当事者間で共有秘密を確立し、適切な相互認証、データ暗号化、及びデータ完全性の保護が実現される。これは以下に詳述するように、様々な方法で達成することができる。一例として、リモートデバイス（たとえばサーバ）にほぼ同期され、文字列を生成する認証トークンを用いて共有秘密を確立する方法がある。文字列とは、たと

えば秘密コードや乱数により暗号化された時刻に基づくパスワードである。文字列は、ローカルデバイス（たとえばワークステーション）に伝達されると所定の関数を用いて変更され、結果（たとえば第二文字列）が生成される。この結果はリモートデバイスに送信される。受信後、リモートデバイスは、認証トークンにより生成された元の文字列と関連し、一致する可能性のある有限個の文字列の値を結果と比較する。次に、リモートデバイス及びユーザのローカルデバイスは、一致する値または一致する値の関数を秘密として共有し、両者間で伝達される情報の暗号化及び情報の完全性の強化、または相互認証の実行、もしくはその両方を行う。あるいは、リモートデバイス及びローカルデバイスが両者の共有秘密を用いて、より大きな（ということは、より安全な）秘密を確立し、この秘密を用いてデータの暗号化、両者間で転送される情報の完全性の強化、及び相互認証のいずれか、あるいはそれらの全てを実行する。

【００１９】

図１は、本発明に係る認証トークンを用いて共有秘密を確立するためのシステム１００を示している。システム１００はワークステーション１２０、サーバ１３０、１４０及び１５０、ネットワーク１６０並びに認証トークン１７０を備える。当業者には、システム１００がワークステーション、サーバ、及び他のネットワーク構成装置を含み得ることが理解されるであろう。

【００２０】

ワークステーション１２０は、ネットワーク１６０との間でデータの送受信を行うことのできるコンピュータである。ワークステーション１２０は、プロセッサ、メモリ、及び人間とのインタラクションを可能にする入力／出力装置（図示せず）から構成される。ワークステーション１２０は、本明細書で説明される認証技術を実行するソフトウェア、たとえば暗号化ソフトなどを備える。更に、ワークステーション１２０は、ネットワーク１６０を介してデータを転送するために、モデム（図示せず）または他の通信装置を備える。当業者には、本明細書で説明される実施形態に係る構成のいずれもが、ワークステーション１２０に含まれ得ることが理解されるであろう。たとえば、ワークステーション１２０は外部メモリに格納されたソフトウェアを利用して、本明細書で説明される認証技術を

実行する。
【００２１】
サーバ１３０、１４０及び１５０は、認証を目的として複数のネットワーク装置と交信するワークステーション１２０の性能を示すために、図１に呈示したものである。各サーバは、ネットワーク１６０との間でデータの送受信を行うことのできるコンピュータである。各サーバを、アプリケーションに応じて個別に構成し、別々のエンティティによって制御することも可能である。たとえば銀行の場合、サーバ１３０を操作して顧客の金融データにリモートでアクセスすることができる。サービス業の企業の場合は、サーバ１４０を操作して顧客の口座情報にリモートでアクセスすることができる。更に、製造業者はサーバ１５０を操作して、顧客が注文商品の出荷状況に関する情報にアクセスできるようにすることも可能である。これらの各サーバは、特定の人だけに知らされる情報のアクセスを記憶且つ制御することができる。それを実現するために、本明細書で説明される認証技術のいずれか１つまたは複数を用いて、意図した相手のみが特定の情報を受信できるようにすることも可能である。
【００２２】
ネットワーク１６０は、インターネットなどの通信媒体であり、その媒体に接続された装置間で情報を回送させるものである。図１はネットワーク１６０に接続されたコンピュータを示しているが、通信機能を備えた他の構成装置も同様にネットワーク１６０に接続可能である。本明細書では、便宜上、ネットワーク１６０がインターネットを指すものとし、インターネットのユーザ認証が認証トークンを用いてどのように行われるかを示す。しかしながら、本発明に係る認証技術は、他のWANやローカルエリアネットワーク（LAN）、ネットワークプロトコル、及び他の通信媒体に用いることも可能である。
【００２３】
認証トークン１７０は、入力（たとえばキーパッド、ライトペンなど）及び出力機能（たとえば液晶ディスプレー、スピーカーなど）を備える。入力機能により、文字列などの情報が認証トークン１７０に伝達される。その情報は、出力機能によりユーザまたは別の装置に伝達される。認証トークンには、リモートデバ

イスと同期化されているもの（時間同期方式トークン）や、キーパッドで入力された文字列を処理してレスポンスを生成するよう構成されているもの（チャレンジ＆レスポンス方式トークン）、または適切な読取装置を介することによりアクセス可能となる情報を格納するよう設計されたもの（スマートカード）などがある。これらの操作を行うために、認証トークン１７０はプロセッサ及びメモリ（図示せず）を備えるのが望ましい。更に、認証トークン１７０は、操作用の起動コード（ＰＩＮまたはバイオメトリクス）を要求するよう構成される。認証トークン１７０は、ワークステーション１２０に対して物理的に接続されるか否かに関わらず、システム１００の一部を成し、以下に詳述する認証技術を実行するものである。

【００２４】

図２は、本発明に係る認証トークンを用いて共有秘密を確立する方法を示す。この方法では、まず認証トークンを提供する（工程２００）。認証トークンには時間同期方式トークンやチャレンジ＆レスポンス方式トークンがあり、本明細書で説明される認証技術を実行するために構成されたトークンであれば、いずれも使用可能である。認証トークンは共有秘密を確立するために利用される（工程２２０）。共有秘密を確立するための技術を、図３～図８に基づいて以下に説明する。

【００２５】

図３ａは、本発明に係る時間同期方式の認証トークンとハッシュ関数を用い、共有秘密を確立する方法を示す。従来の方法では、ユーザがワークステーションに文字列を入力すると、ワークステーションは文字列を暗号化されない状態でサーバに転送する。本発明の実施例においては、文字列が暗号化されない状態で送信されることはない。むしろ、この実施例では、認証トークンで表示された文字列を用いて通信者間に共有秘密を生成し、妥当なレベルの認証と安全なセッションを実現する。

【００２６】

まず、時間同期方式トークン１７０で文字列が生成される（工程３００）。この文字列は、トークンとサーバのみが認識する秘密コードにより分単位の時刻を

暗号化したものであることが望ましい。次に、この文字列はワークステーション１２０に伝達される（工程３１０）。たとえば、ユーザはその文字列を読み取り、ワークステーションに手動で入力することができる。あるいは、ワークステーションと認証トークンが接続されている場合、ワークステーションはその文字列を認証トークンから自動的に読み取ることができる。文字列を受信後、ワークステーションは市販のハッシュプログラムを実行し、受信した文字列のハッシュ（ｈ（文字列））を生成する（工程３２０）。このハッシュは暗号化用の一方向関数であり、任意サイズの入力データを取得して固定サイズの出力データを生成する。ワークステーションはｈ（文字列）をサーバ１３０に送信する（工程３３０）。

【００２７】

トークンが直前の７分間または直後の３分間に表示した文字列（または分数に応じた他の適切な値）に基づき、サーバは複数の文字列からいずれか１つを受け入れる。これは、タイピングや転送におけるクロックのスキューや遅延を許容するためである。受け入れ可能な文字列の個数が少ないために、サーバは受け入れ可能な各文字列のハッシュを容易に演算し、各ハッシュを受信されたハッシュであるｈ（文字列）と比較することにより、演算されたハッシュから一致するハッシュを一義化する（工程３４０及び３５０）。一致するハッシュが見つからない場合、認証は失敗する（工程３６０）。一致するハッシュが見つかった場合は、サーバ及びワークステーションは文字列の関数（文字列のハッシュ、文字列そのもの、または他の変数）を共有秘密として用いる（工程３７０）。つまり、サーバ及びワークステーションは、一致する文字列の関数を用い、ネットワーク１６０上で相互に送信されるメッセージを暗号化する。一致する文字列が盗聴から保護されるのに十分なビットを有している場合には、この技術は有効である。大部分の種類のトークンでは、生成される文字列はあまりに短い（わずか2^{32}通りの値しか表すことができない）。しかし、文字列が短すぎると、盗聴者がｈ（文字列）を捕獲し、徹底的な探索によって文字列を特定することが可能となってしまう。

【００２８】

図３ｂは、本発明の図３ａに示された例に類似した実施例を示す。この実施例は図３ａの工程３００～３２０を含む。しかしながら、図３ｂの実施例においては、図３ａの工程３３０に示されるように文字列の完全なハッシュをサーバに送信するのではなく、ハッシュされた文字列の数ビットのみ（たとえば、６４ビットの文字列のハッシュから１２ビット）をサーバに送信する（工程３３５）。文字列のハッシュをサーバに送信する目的は、（文字列を特定するのに必要な文字列が１０個のみのクロックスキューを想定した場合）サーバ１３０が１０個前後の受け入れ可能な文字列から正しい文字列を特定することである。サーバ１３０は少数の文字列を区別するだけで済むため、ハッシュされた文字列の数ビットにより、サーバ１３０は残り９個の文字列のいずれにも衝突しないハッシュ文字列を高い確率で演算することができる。

【００２９】

完全なメッセージダイジェストではなく、ハッシュされた文字列の数ビットのみを送信するのは、盗聴者が文字列に該当する可能性のあるものを探索し、その中（2^{64}通り）から文字列を絞り込むのを阻止するためである。たとえば、ワークステーション１２０が８ビットのハッシュを送信する場合、およそ2^{56}通りの文字列がこのハッシュと一致するため、盗聴者が正しい文字列を特定するには2^{56}通りの値を探索しなくてはならない。

【００３０】

ワークステーションが８ビットのハッシュ文字列を送信し、元の文字列がランダムな６４ビットのデータを有する場合、１０個ある文字列のうちの２個以上がユーザの入力した文字列のハッシュと一致する確率は$1-(255/256)^9$％、つまり約４％である。（他９個の文字列の１つが元の文字列と同じ文字列にハッシュし、サーバが誤った文字列を推測してしまうため）認証を40回試行する中で約1回の失敗も容認されない場合、ワークステーションは１６ビットのハッシュを送信することができる。それでも、盗聴者には探索しなくてはならない値が2^{48}通り残される。

【００３１】

文字列のハッシュの数ビットのみを受信した後、サーバは受け入れ可能な複数

の文字列の値について各々のハッシュを演算し、演算したハッシュと受信した元のハッシュとを比較する（工程３４５）。この比較に基づき、サーバは受信したビットが受け入れ可能な文字列の値と一致するか否かを判定する（工程３５５）。演算したハッシュ及び受信したビット間に全く一致が見られない場合、認証の試行は失敗する（工程３６０）。一致が見られた場合、サーバは受け入れ可能な値の中で受信したビットと一致するものが複数個あるか否かを判定する（工程３６５）。一致する値が１つのみの場合は、サーバ及びワークステーションは文字列の関数（たとえば、文字列のハッシュ、文字列そのもの、または他の変数）を共有秘密として用いる（工程３７０）。一致する値が複数個ある場合は、サーバは文字列のハッシュを一義化せよとの命令をワークステーションに送信する（工程３７５）。この例では、できるだけ少ない情報を通信しながら、受け入れ可能な値が１つに特定される。このような技術について以下に説明する。

【００３２】

認証の試行の失敗を防ぐには、受信されたハッシュと一致する所定の文字列が複数個あることをサーバに認識させ、ハッシュ内にビットを追加するよう要求すればよい。サーバは一致する文字列の全ての候補を把握しているため、衝突した文字列を差異化すると思われるハッシュを認識し、そのハッシュ内の特定のビットを要求する（つまり、必要なビットを求める命令をワークステーションに送信する）ことができる。あるいは、サーバが「次のｋビット」を要求する方法もある。ワークステーションが保有する元の文字列を特定するのに必要なビット数をサーバが受信する際、特定のビットを要求することにより、サーバが受信するビットは可能な限り少数で済むことになる。

【００３３】

また、上述の技術の代わりに、ワークステーションがハッシュされた文字列のビットを初めからサーバに全く送信しないで、むしろサーバが１０個の所定の文字列をチェックし、その１０個の文字列を差異化する最短のビット数を要求するようにしてもよい。また、この技術に変更を加え、サーバが定数を演算するようにすることもできる。この定数は、衝突した所定の各文字列と共にハッシュ化される際に、別のハッシュを生成する。この場合、サーバは定数をワークステーショ

ンに送信し、生成されるハッシュを要求する。次に、ワークステーションが関数を用いて文字列と共に定数をハッシュ化（文字列｜定数）すると、結合ハッシュ文字列がサーバに送信され、所定の文字列と照合される。サーバは、一致する文字列から元の文字列を算出し、ワークステーションとの間で共有秘密として利用する。上述の認証技術を用いる際には、結合された情報（文字列のハッシュと定数）から文字列を特定するのに十分な情報が、盗聴者には提供されないことをユーザは確信するはずである。

【００３４】

他に、一致する受け入れ可能な値を特定（一義化）する実施例としては、サーバが（たとえばＰＩＮと連結した文字列のハッシュの数ビットを受信した後に）ワークステーションに値を送信する方法がある。ワークステーションは、サーバに認識された関数を用い、（サーバから送信された）元の値、及びＰＩＮと連結した（認証トークンから送信された）文字列の関数を表す出力値を生成する。生成された出力値はサーバに送信され、受け入れ可能な値を１つに特定するために用いられる。

【００３５】

いったん共有秘密が確立されると、サーバ及びワークステーションは相互認証を容易に実行することができる。共有秘密に基づいた相互認証を実行するための技術には周知のものが幾つかあり、それらのいずれかを必要に応じて用いる。これらの技術については、『ネットワークセキュリティ』の第２２３頁に説明されている。たとえば、サーバはワークステーションが共有秘密を有していることを証明する方法を実行することができる。この方法では、まずサーバからワークステーションに第二文字列を伝達し、共有秘密及び第二文字列、またはそれらのいずれか一方を用いた関数（係る秘密及び第二文字列のハッシュなど）を実行し、出力データを生成する。次に、ワークステーションが出力データをサーバに送信すると、サーバはその出力データを期待値と比較し、ローカルデバイスが共有秘密を有していることを証明する。この過程をそのまま逆にして、ワークステーションがサーバを認証することも可能である。

【００３６】

サーバが文字列（または受け入れ可能な文字列の小さな集合）について証明した後で、文字列の特定に用いられる情報がワークステーションにより明示されるようにするのが望ましい。そうしないと、中間サーバまたは偽装サーバの使用者がプロトコルに従って操作し、徹底的に探索して正しい値を見つけ、セッションを継続することが可能となってしまう。このことは本発明の実施例すべてに該当するため、ワークステーションが係る情報を明示する前に、サーバが文字列について証明するようにすることが推奨される。

【００３７】

図４ａは、本発明に係る時間同期方式の認証トークン、ハッシュ関数、及びＰＩＮを用いて共有秘密を確立する方法を示す。この方法では、トークンによって生成される文字列が短すぎる場合に徹底的な探索による被害を回避することが可能である。

【００３８】

まず、時間同期方式トークン１７０で文字列が生成される（工程４００）。次に、文字列がＰＩＮと共にワークステーション１２０に伝達される（工程４１０）。たとえば、ユーザが文字列を読み取り、ワークステーションにＰＩＮと共に手動で入力することができる。または、ワークステーションが認証トークンに接続されている場合、ユーザがワークステーションにＰＩＮを入力すると、ワークステーションは認証トークンから文字列を自動的に読み取ることができる。文字列を受信後、ワークステーションは市販のハッシュプログラムを実行し、文字列及びＰＩＮのハッシュ（ｈ（文字列｜ＰＩＮ）を生成する（工程４２０）。次に、ワークステーションはｈ（文字列｜ＰＩＮ）をサーバ１３０に送信する（工程４３０）。さらに、サーバ１３０は認識済みのＰＩＮを用い、受け入れ可能な複数の文字列の各々についてｈ（文字列｜ＰＩＮ）を演算し、受け入れ可能な文字列をワークステーション１２０から受信したｈ（文字列｜ＰＩＮ）と比較する（工程４４０及び４５０）。一致するものがない場合、認証の試行は失敗する（工程４６０）。一致するものがある場合は、サーバ及びワークステーションは文字列及びＰＩＮの関数（たとえば、定数に連結されたＰＩＮに連結された文字列のハッシュ）を共有秘密として用いる（工程４７０）。

【００３９】
図４ｂは、本発明の図４ａに基づいた上述の例に類似した実施例を示す。この実施例の工程４００～４２０は図４ａに類似しているが、それ以降の工程はｈ（文字列｜ＰＩＮ）のビット数を限定して送信する点で異なる（工程４３５）。ｈ（文字列｜ＰＩＮ）の数ビットのみを受信した後、サーバはＰＩＮに連結された受け入れ可能な複数の文字列の値について各々のハッシュを演算し、演算したハッシュと受信したビットを比較する（工程４４５）。この比較に基づき、サーバは受信したビットが受け入れ可能な文字列の値と一致するか否かを判定する（工程４５５）。演算したハッシュ及び受信したビット間に一致するものが全くない場合、認証の試行は失敗する（工程４６０）。一致が見つかった場合、サーバは受け入れ可能な値の中で受信したビットと一致するものが複数個あるか否かを判定する（工程４６５）。一致する値が１つしかない場合、サーバ及びワークステーションは文字列の関数（たとえば、定数と連結されたＰＩＮに連結された文字列のハッシュ）を共有秘密として用いる（工程４７０）。一致するものが複数個ある場合は、サーバはＰＩＮに連結された文字列のハッシュを一義化せよとの命令をワークステーションに送信する（工程４７５）。文字列のハッシュのビットを適量だけ用いることにより、一致する受け入れ可能な値が１つに特定される。これは、図３ｂを参照して上述した技術のいずれか１つまたは複数を利用することによって達成可能である。
【００４０】
上記の実施例では、ワークステーション及びサーバ間での共有秘密は、ｈ（文字列｜ＰＩＮ）とは異なる。たとえば、ワークステーションからサーバに送信されるハッシュ文字列がＳＨＡ（文字列｜ＰＩＮ）であり、共有秘密がワークステーション及びサーバで認識済みの定数を伴うＳＨＡ（文字列｜ＰＩＮ｜定数）である場合もある。（ＳＨＡとは、「安全なハッシュアルゴリズム」（secure hash algorism）、すなわち米国標準技術協会（ＮＩＳＴ）が提案するメッセージダイジェスト機能の略語である。）この認証技術は、ＰＩＮと併せた文字列が盗聴者による探索をかわすに足るビット（たとえば６４ビット以上）を有する場合、全ての時間同期方式トークンにおいて有効である。

【００４１】
図５ａ～５ｃは、本発明に係る時間同期方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。この実施例においては、ワークステーション及びサーバ間で共有された秘密（たとえば文字列）が一義化されるのは、共有秘密鍵交換プロトコルを実行する前、共有秘密鍵交換プロトコルを実行する間、または共有秘密鍵交換プロトコルを実行した後である。
【００４２】
図５ａは、共有秘密鍵交換プロトコルを実行する前に、共有秘密を一義化する方法を示す。この方法では、まず文字列を同期トークン１７０に表示する（工程５００）。次に、ユーザはその文字列をワークステーション１２０に入力する（工程５１０）。ワークステーション及びサーバは、前記の各実施形態で説明したように、その文字列を用いて第一共有秘密を確立する（工程５２０）。続いて、この第一共有秘密を用い、ベロヴィン・メリット共有秘密鍵交換プロトコルなどの共有秘密鍵交換プロトコルを使用して、より強力な共有秘密（たとえば、より多くのビットを有する共有秘密）を確立することができる（工程５３０）。より強力な共有秘密がいったん確立されると、それを用いてトラフィックが暗号化されるか、または他の操作が実行される（工程５４０）。
【００４３】
図５ｂは、共有秘密鍵交換プロトコルを実行しながら共有秘密を一義化する方法を示す。この方法は、図５ａで示された方法に類似しているが、図５ｂにおいて工程５２０及び５３０は結合される（工程５２７）。共有秘密鍵交換プロトコルの実行に伴って第一共有秘密を一義化することのできる技術は幾つかある。そうした技術の１つに「ベロヴィン・メリット共有秘密鍵交換プロトコル」の使用がある。これは、ワークステーション１２０において共有秘密鍵交換プロトコルの第一暗号化メッセージに定数を連結させ、サーバ１３０においては解読後のメッセージに適正なハッシュビットが含まれていることを確認させるものである。他には、ワークステーション１２０において認証トークンからの文字列のハッシュの一部または全部を暗号化前のメッセージに連結させ、サーバ１３０においては解読後のメッセージに適正なハッシュビットが含まれていることを確認させる

技術もある。更には、暗号化されていない文字列のハッシュビットの一部または全部を、暗号化メッセージと併せてワークステーション１２０に送信させる技術もある。

【００４４】

あるいは、図５ｃに示されるように、認証トークンからの文字列を一義化しないまま第一共有秘密として用い、共有秘密鍵交換プロトコルを実行してもよい（工程５２５）。続いて、この文字列を一義化し（工程５３５）、共有秘密鍵交換プロトコルによって確立されたより強力な共有秘密を特定することができる（工程５４０）。

【００４５】

たとえば、変形版ベロヴィン・メリット共有秘密鍵交換プロトコルを実行すると、サーバはワークステーションからの文字列と共に暗号化された第一メッセージを受信し、鍵の一部を選択してから、その文字列に対応する受け入れ可能な数個の値に基づき、完全な鍵に対応する値を幾つか算出し、（暗号化されていない）鍵の一部と併せて完全な鍵のハッシュをワークステーションに送信する。次に、ワークステーションは完全な鍵を特定し、そのハッシュをサーバから受信したハッシュと比較する。一致するハッシュがある場合、サーバは（小さな集合の範囲内で）文字列を特定する。この時点で、ワークステーションがその文字列または第二共有鍵を有していることを、チャレンジ＆レスポンス（チャレンジは前のメッセージと併せてサーバから任意に送信される）を通じてワークステーション自身が証明する。

【００４６】

上記の技術を援用し、送信されるハッシュビット数を最小限に抑えながら（たとえば、サーバにより多くのビットを要求させるか、またはハッシュに含まれるはずの定数を送信させ、衝突を回避するなどして）共有秘密を確立すること、または認証試行の失敗を回避することができる。共有秘密鍵交換プロトコルのベースとして用いられる文字列の長さは、３２ビットを超えることが必要である。３２ビット以下の場合には、より確実な認証が行えるよう、その文字列にＰＩＮが追加された後に共有秘密鍵交換プロトコルが実行される。

【００４７】
図６は、本発明に係るチャレンジ＆レスポンス方式の認証トークンを用いて共有秘密を確立する方法を示す。この方法では、まずサーバ１３０がチャレンジ（文字列）をワークステーション１２０に送信する（工程６００）。受信後、ユーザはそのチャレンジをチャレンジ＆レスポンス方式の認証トークンに入力する（工程６１０）。認証トークンは入力されたチャレンジを処理し、レスポンスを生成する（工程６２０）。次に、生成されたレスポンスはワークステーション１２０に送信され（工程６３０）、ワークステーション及びサーバ間で共有秘密として用いられる（工程６４０）。この認証技術は、レスポンスの長さが十分ある（３２ビットを超える）場合には、ワークステーション及びサーバ間において高レベルの認証を実現する。長さが十分になければ、図７に関する下記説明のように、この実施例に変更を加えて認証レベルを高めることができる。
【００４８】
図７は、本発明に係るチャレンジ＆レスポンス方式の認証トークン及びＰＩＮを用いて共有秘密を確立する方法を示す。この方法では、まずサーバ１３０がワークステーション１２０にチャレンジを送信する（工程７００）。受信後、ユーザはそのチャレンジをチャレンジ＆レスポンス方式の認証トークンに入力する（工程７１０）。次に、認証トークンは入力されたチャレンジを処理し、レスポンスを生成する（工程７２０）。さらに、ユーザは生成されたレスポンスをＰＩＮと併せてワークステーション１２０に入力する（工程７３０）。そうすると、ワークステーション１２０及びサーバ１３０は、レスポンス及びＰＩＮの関数を共有秘密として用いることができる（工程７４０）。この実施例では、レスポンス及びＰＩＮの長さがセッション鍵に対して十分な（３２ビットを超える）場合に、高レベルの認証を実現する。
【００４９】
図８は、本発明に係るチャレンジ＆レスポンス方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。初めに、サーバ１３０がワークステーション１２０にチャレンジを送信する（工程８００）。受信後、ユーザはチャレンジ＆レスポンス方式の認証トークンに、チャレンジ及び場

合によりＰＩＮを入力する（工程８１０）。次に、認証トークンは入力されたチャレンジを処理し、レスポンスを生成する（工程８２０）。ユーザがそのレスポンスをワークステーション１２０に入力する（工程８３０）と、そのレスポンスを用いて共有秘密鍵交換プロトコルが実行される（工程８４０）。ワークステーション１２０とサーバ１３０とは共に、鍵交換により特定された秘密を共有秘密として用いる（工程８５０）。あるいは、レスポンスの関数（たとえば別のＰＩＮと併せたレスポンスのハッシュなど）を鍵交換に用いて、ワークステーション１２０及びサーバ１３０間での認証をより確実なものにすることも可能である。

【００５０】

図９ａ～９ｃは、本発明に係るスマートカードを用いて共有秘密を確立する方法を示す。具体的には、図９ａは、本発明に係るスマートカードを用いてローカルデバイス及びリモートデバイス間に共有秘密を確立する方法を示す。この方法では、まずスマートカードを提供する（工程９００）。このスマートカードは起動コードにより起動する。この起動コードにはＰＩＮ、バイオメトリクス、または他の形態の入力データがある。また、スマートカードはデータ処理用の内部クロックを備えるか、または外部クロック（たとえばワークステーションのクロックなど）を用いて動作する。いったん起動すると、カードはデータ（たとえば文字列など）をワークステーションなどのローカルデバイスに伝達する（工程９２０）。ワークステーションは、カードリーダーを通じて、または直接的に内部受信機及び適切なソフトウェアを用いてデータを受信するよう構成されている。

【００５１】

データ受信後、ワークステーションは時間同期方式またはチャレンジ＆レスポンス方式の認証トークンに関する上記技術のいずれか１つを用い、受信したデータを使用してサーバなどのリモートデバイスとの間に共有秘密を確立することができる（工程９４０）。たとえば、ワークステーションが第一文字列を生成してリモートデバイスに伝達すると、その第一文字列はリモートデバイスにおいて受け入れ可能な複数個の値のいずれか１つと一致する。共有秘密を確立するには、第一文字列をリモートデバイスからワークステーションに伝達し、その第一文字列をワークステーションで処理して生成した第二文字列を、共有秘密として用い

ることもできる。その共有秘密の使用により、ユーザ認証、データ暗号化、及びデータ完全性の保護が実現される。

【００５２】

図９ｂは、スマートカード及びリモートデバイス間で共有秘密を確立し、ローカルデバイスとの間でその秘密を共有する方法を示す。この方法では、まずスマートカードを提供する（工程９０２）。図９ａに関する上記説明のように、スマートカードは起動可能であり、内部クロックまたは外部クロックを使用する。更に、スマートカードは、リモートデバイスとの通信を速やかに行うための通信用ソフトウェア及びハードウェアを備える。リモートデバイスと交信するために、スマートカードは上記技術（スマートカードが認証トークン及びワークステーションとして動作し、リモートサーバとの間に共有秘密を確立する）の１つまたは複数を利用し、リモートデバイスとの間に共有秘密を確立する機能を有する（工程９２２）。たとえば、スマートカードが第一文字列を生成してリモートデバイスに伝達すると、その第一文字列はリモートデバイスにおいて受け入れ可能な複数の値のいずれか１つと一致する。共有秘密を確立するには、第一文字列をリモートデバイスからスマートカードに伝達し、その第一文字列をスマートカードで処理して生成した第二文字列を、共有秘密として用いることもできる。その後、スマートカードはその共有秘密をワークステーションに伝達し、ユーザ認証、データ暗号化、及びデータ完全性の保護が実現される（工程９４２）。

【００５３】

図９ｃは、リモートデバイス及びローカルデバイス間でのトランザクション用にスマートカードを使用し、スマートカード及びリモートデバイス間で共有秘密を確立する方法を示す。この方法では、まずスマートカードを提供する（工程９０４）。図９ａに関する上記説明のように、スマートカードは起動可能であり、内部クロックまたは外部クロックを使用する。更に、スマートカードは、リモートデバイスとの通信を速やかに行うための通信用ソフトウェア及びハードウェアを備える。リモートデバイスと交信するために、スマートカードは上記技術の１つもしくは複数を利用し、リモートデバイスとの間に共有秘密を確立する機能を有する（工程９２４）。いったん共有秘密が確立されるとスマートカードはワー

クステーションに共有秘密を伝達しないという点で、この方法は図９ｂに基づいて説明された方法とは異なる。つまり、スマートカード及び共有秘密は、リモートデバイス及びローカルデバイス間でのトランザクションに利用されるが、共有秘密はローカルデバイスに対しては明かされないままとなる（工程９４４）。

【００５４】

本発明の実施例は、適切な認証を実現し、通信媒体を介して当事者間で伝送される情報の完全性を高めるものである。本明細書で説明された認証技術により、ユーザは、使用するトークンの種類及びワークステーションやサーバで使用可能なソフトウェアに応じて、認証レベルをカスタマイズすることができる。たとえば、ワークステーション且つサーバが共に、ハッシング及び暗号化用のソフトウェアしか備えていない場合でも、上記技術を利用すれば、これら２種類のソフトウェア及び認証トークンを備えるだけで、ワークステーション及びサーバにおいて高度な認証を行うことが可能である。

【００５５】

以上、本発明の実施形態について説明したが、本発明の適正な範囲から外れることなく、様々の変形例が可能であること、また同等物をもって代用できることは、当業者には理解されるであろう。

更に、本発明の主旨から外れることなく様々の変更を加え、特定の要素、技術、及び実施形態を本発明の教示に応用することも可能である。従って、本発明の範囲は、本明細書で開示した特定の実施形態や方法に限定されるものではなく、請求の範囲に該当する実施形態の全てを包含するものである。

【図面の簡単な説明】

【図１】

本発明に係る認証トークンを用いて共有秘密を確立するシステムを示す。

【図２】

本発明に係る認証トークンを用いて共有秘密を確立する方法を示す。

【図３ａ】

本発明に係る時間同期方式の認証トークン及びハッシュ関数を用いて共有秘密を確立する方法を示す。

【図３ｂ】
本発明に係る時間同期方式の認証トークン、ハッシュ関数、及び文字列の限定されたビット数を用いて共有秘密を確立する方法を示す。
【図４ａ】
本発明に係る時間同期方式の認証トークン、ハッシュ関数及びＰＩＮを用いて共有秘密を確立する方法を示す。
【図４ｂ】
本発明に係る時間同期方式の認証トークン、ハッシュ関数、ＰＩＮ、及び文字列の限定されたビット数を用いて共有秘密を確立する方法を示す。
【図５ａ】
本発明に係る時間同期方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。
【図５ｂ】
本発明の別の実施方法に係る時間同期方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。
【図５ｃ】
本発明の更なる別の実施方法に係る時間同期方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。
【図６】
本発明に係るチャレンジ＆レスポンス方式の認証トークンを用いて共有秘密を確立する方法を示す。
【図７】
本発明に係るチャレンジ＆レスポンス方式の認証トークン及びＰＩＮを用いて共有秘密を確立する方法を示す。
【図８】
本発明に係るチャレンジ＆レスポンス方式の認証トークン及び共有秘密鍵交換プロトコルを用いて共有秘密を確立する方法を示す。
【図９ａ】
本発明に係るスマートカードを用いてローカルデバイス及びリモートデバイス

間に共有秘密を確立する方法を示す。

【図９ｂ】

スマートカード及びリモートデバイス間に共有秘密を確立し、係る秘密をローカルデバイスと共有する方法を示す。

【図９ｃ】

スマートカード及びリモートデバイス間に共有秘密を確立し、リモートデバイス及びローカルデバイス間でのトランザンクション用のスマートカードを用いる方法を示す。

【符号の説明】

１００　認証トークンを用いて共有秘密を確立するためのシステム

１７０　認証トークン

１２０　ワークステーション

１６０　ネットワーク

１３０～１５０　サーバ

【図１】

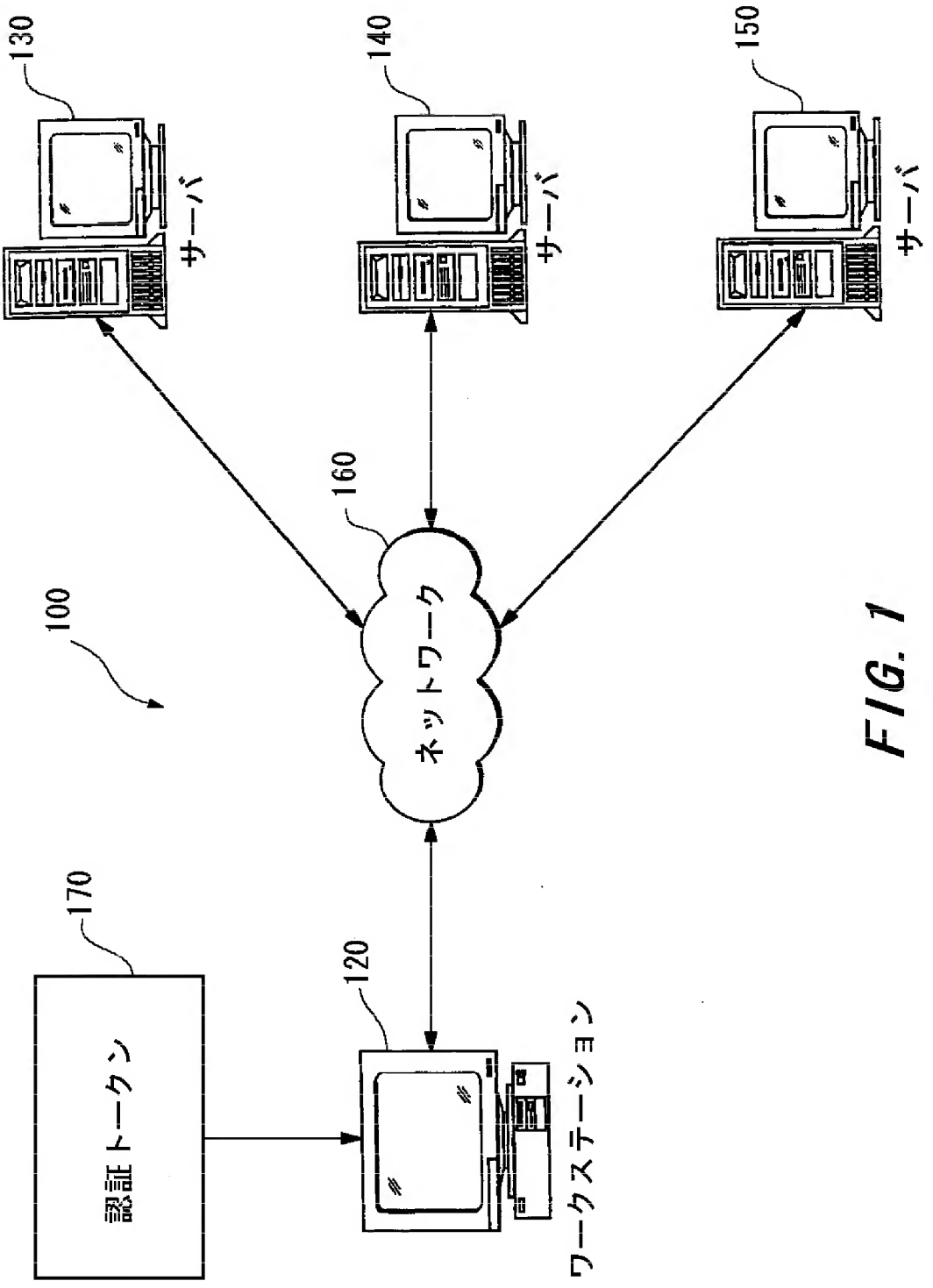

130
サーバ
140
サーバ
150
サーバ
160
ネットワーク
100
170
認証トークン
120
ワークステーション

FIG. 1

【図２】

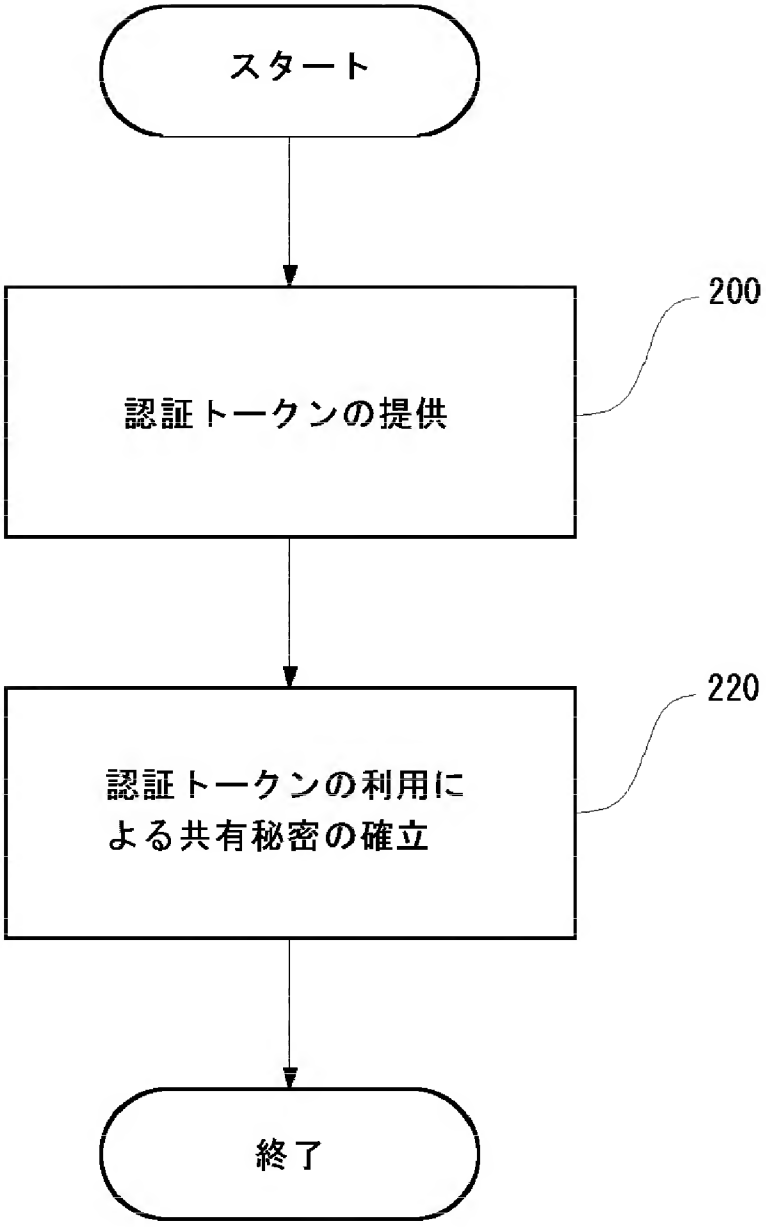


FIG. 2

【図３ａ】

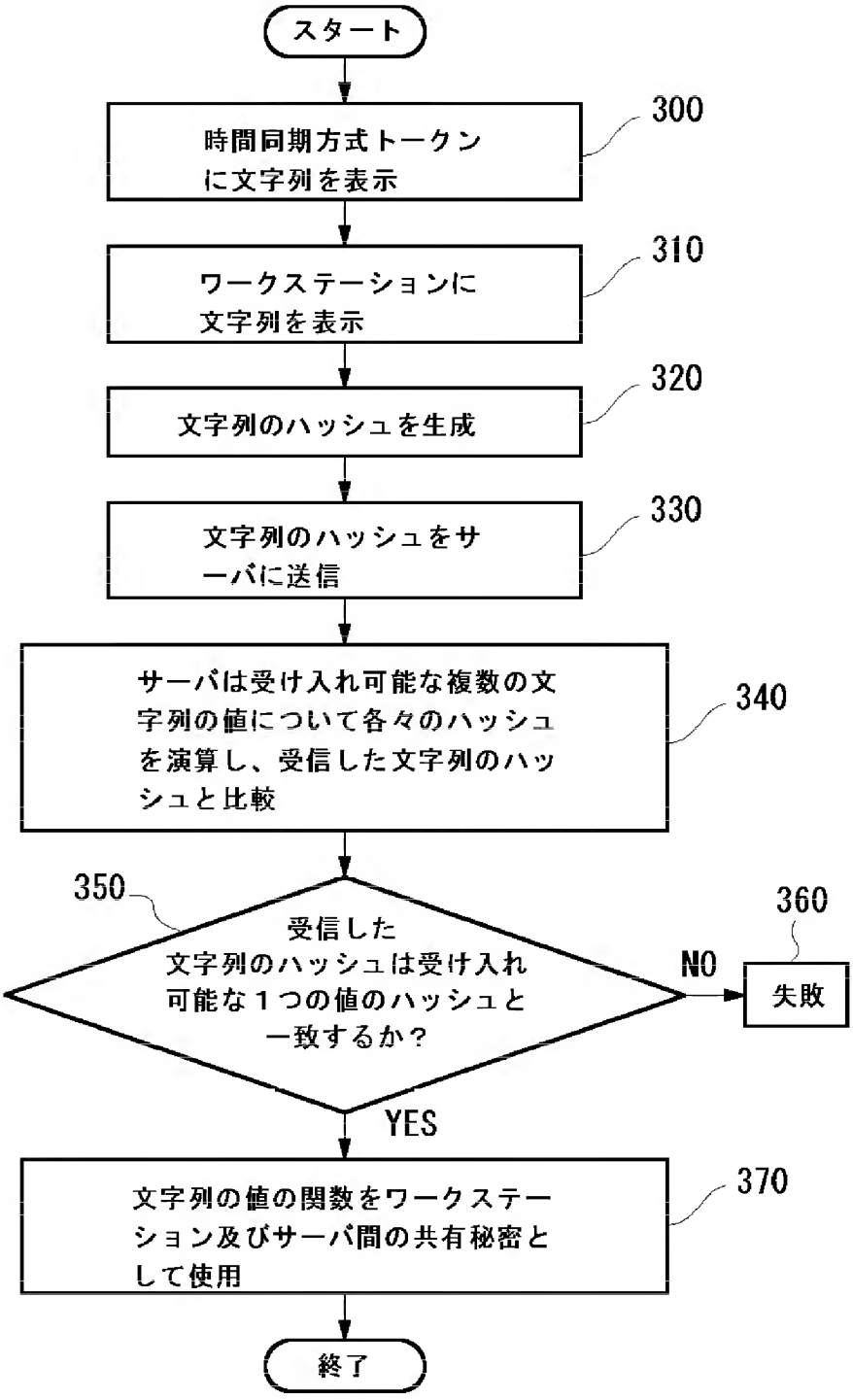

スタート
時間同期方式トークンに文字列を表示
300
ワークステーションに文字列を表示
310
文字列のハッシュを生成
320
文字列のハッシュをサーバに送信
330
サーバは受け入れ可能な複数の文字列の値について各々のハッシュを演算し、受信した文字列のハッシュと比較
340
350
受信した文字列のハッシュは受け入れ可能な１つの値のハッシュと一致するか？
NO
360
失敗
YES
文字列の値の関数をワークステーション及びサーバ間の共有秘密として使用
370
終了

FIG. 3a

【図３ｂ】

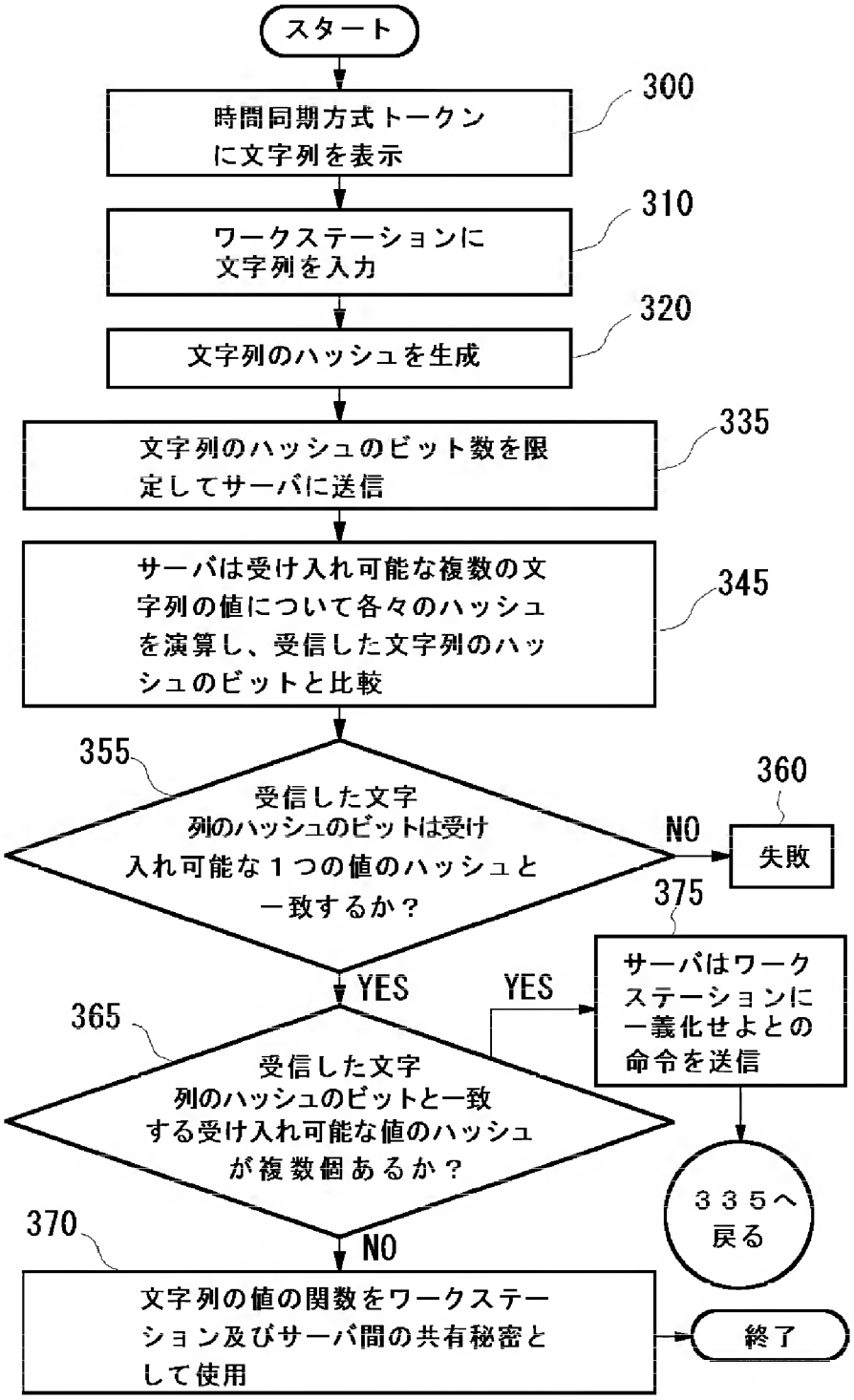

スタート
時間同期方式トークンに文字列を表示
300
ワークステーションに文字列を入力
310
文字列のハッシュを生成
320
文字列のハッシュのビット数を限定してサーバに送信
335
サーバは受け入れ可能な複数の文字列の値について各々のハッシュを演算し、受信した文字列のハッシュのビットと比較
345
355
受信した文字列のハッシュのビットは受け入れ可能な１つの値のハッシュと一致するか？
NO
360
失敗
YES
375
サーバはワークステーションに一義化せよとの命令を送信
YES
365
受信した文字列のハッシュのビットと一致する受け入れ可能な値のハッシュが複数個あるか？
３３５へ戻る
NO
370
文字列の値の関数をワークステーション及びサーバ間の共有秘密として使用
終了

FIG. 3b

【図４ａ】

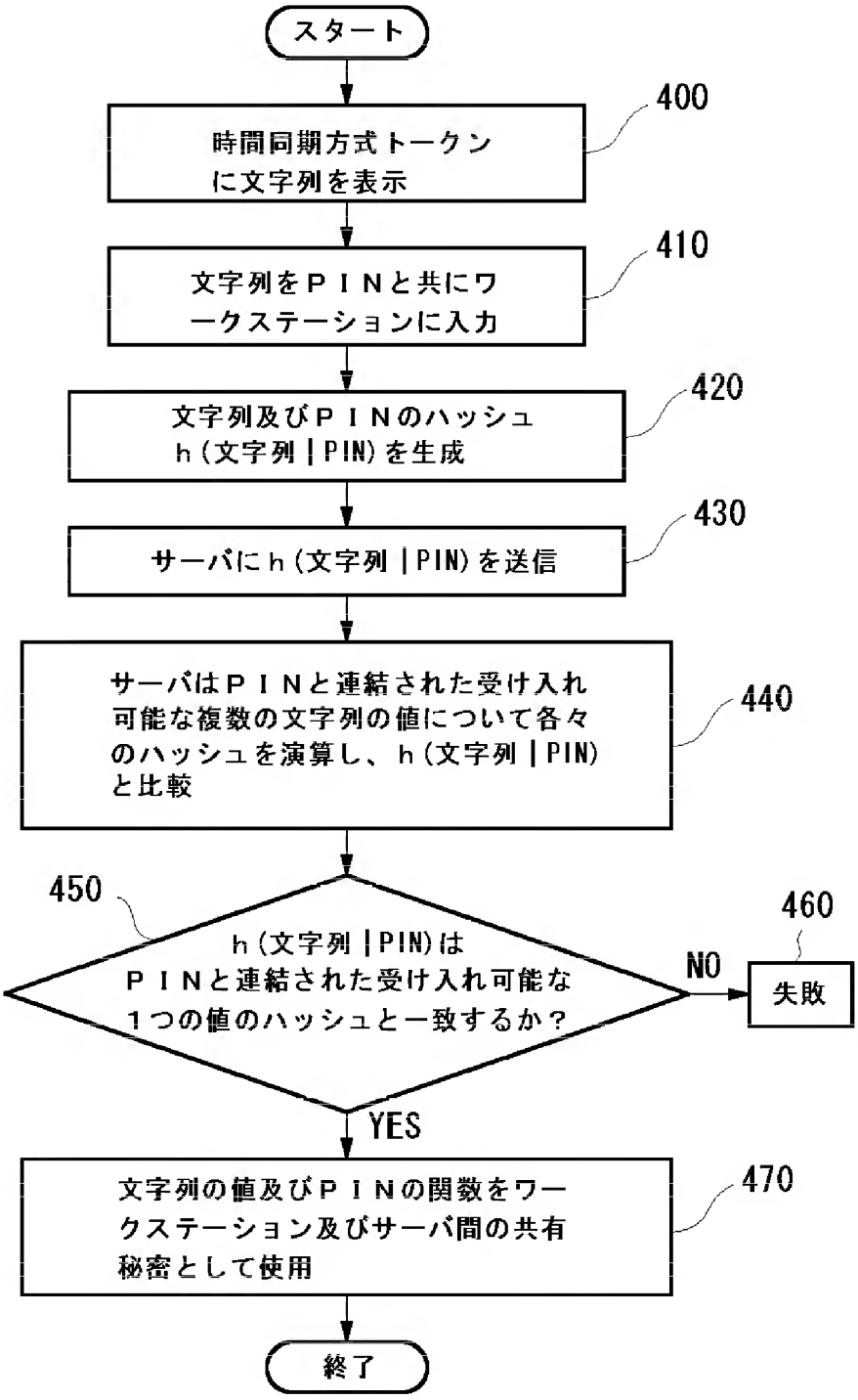

スタート
時間同期方式トークンに文字列を表示
400
文字列をＰＩＮと共にワークステーションに入力
410
文字列及びＰＩＮのハッシュh(文字列|PIN)を生成
420
サーバにh(文字列|PIN)を送信
430
サーバはＰＩＮと連結された受け入れ可能な複数の文字列の値について各々のハッシュを演算し、h(文字列|PIN)と比較
440
450
h(文字列|PIN)はＰＩＮと連結された受け入れ可能な１つの値のハッシュと一致するか？
NO
460
失敗
YES
文字列の値及びＰＩＮの関数をワークステーション及びサーバ間の共有秘密として使用
470
終了

FIG. 4a

【図４ｂ】

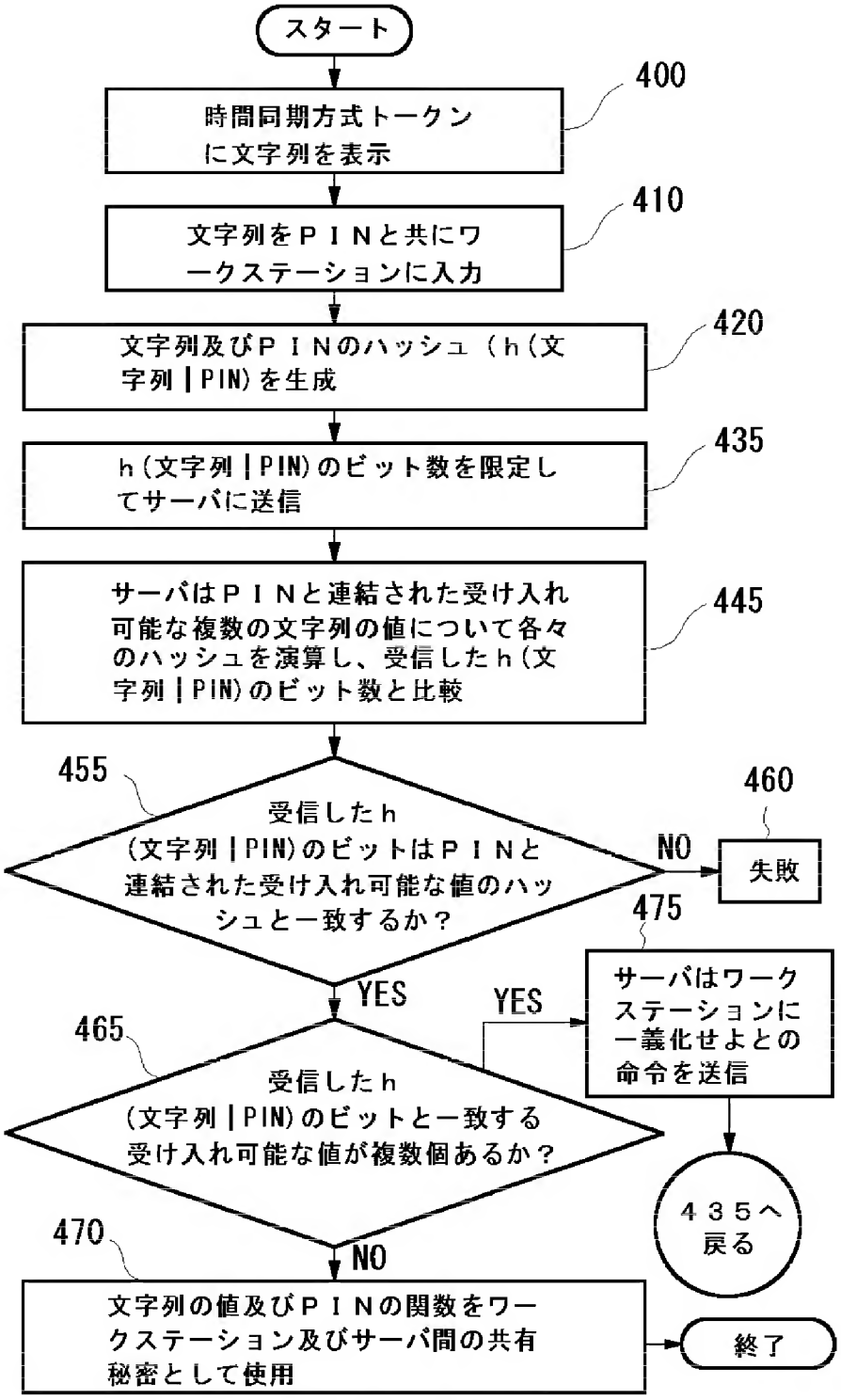

スタート
400
時間同期方式トークンに文字列を表示
410
文字列をＰＩＮと共にワークステーションに入力
420
文字列及びＰＩＮのハッシュ（ｈ(文字列｜PIN)を生成
435
ｈ(文字列｜PIN)のビット数を限定してサーバに送信
445
サーバはＰＩＮと連結された受け入れ可能な複数の文字列の値について各々のハッシュを演算し、受信したｈ(文字列｜PIN)のビット数と比較
455
受信したｈ(文字列｜PIN)のビットはＰＩＮと連結された受け入れ可能な値のハッシュと一致するか？
NO
460
失敗
YES
475
サーバはワークステーションに一義化せよとの命令を送信
YES
465
受信したｈ(文字列｜PIN)のビットと一致する受け入れ可能な値が複数個あるか？
４３５へ戻る
NO
470
文字列の値及びＰＩＮの関数をワークステーション及びサーバ間の共有秘密として使用
終了

FIG. 4b

【図５ａ】

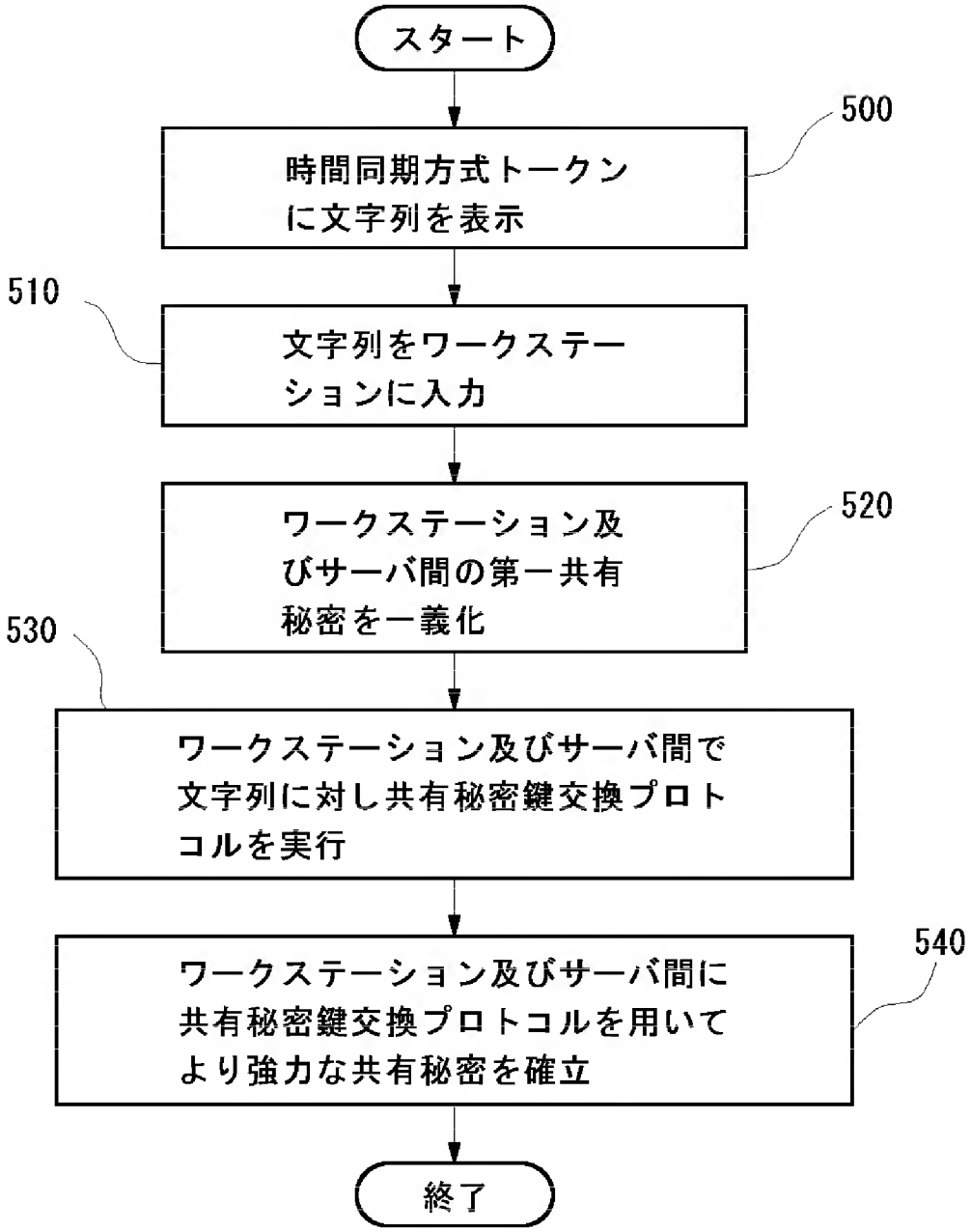

スタート
500
時間同期方式トークンに文字列を表示
510
文字列をワークステーションに入力
520
ワークステーション及びサーバ間の第一共有秘密を一義化
530
ワークステーション及びサーバ間で文字列に対し共有秘密鍵交換プロトコルを実行
540
ワークステーション及びサーバ間に共有秘密鍵交換プロトコルを用いてより強力な共有秘密を確立
終了

FIG. 5a

【図５ｂ】

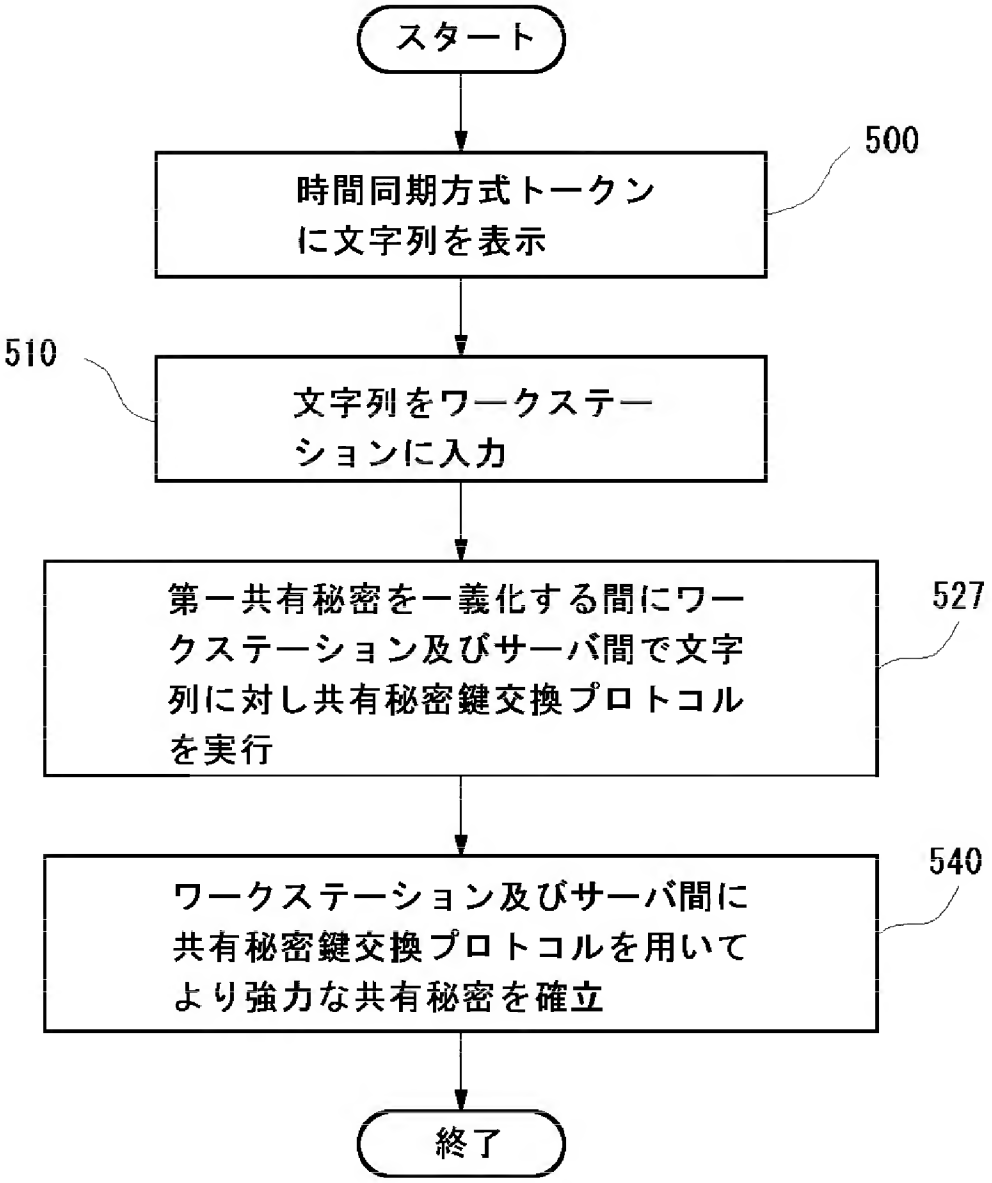

スタート
500
時間同期方式トークンに文字列を表示
510
文字列をワークステーションに入力
527
第一共有秘密を一義化する間にワークステーション及びサーバ間で文字列に対し共有秘密鍵交換プロトコルを実行
540
ワークステーション及びサーバ間に共有秘密鍵交換プロトコルを用いてより強力な共有秘密を確立
終了

FIG. 5b

【図５ｃ】

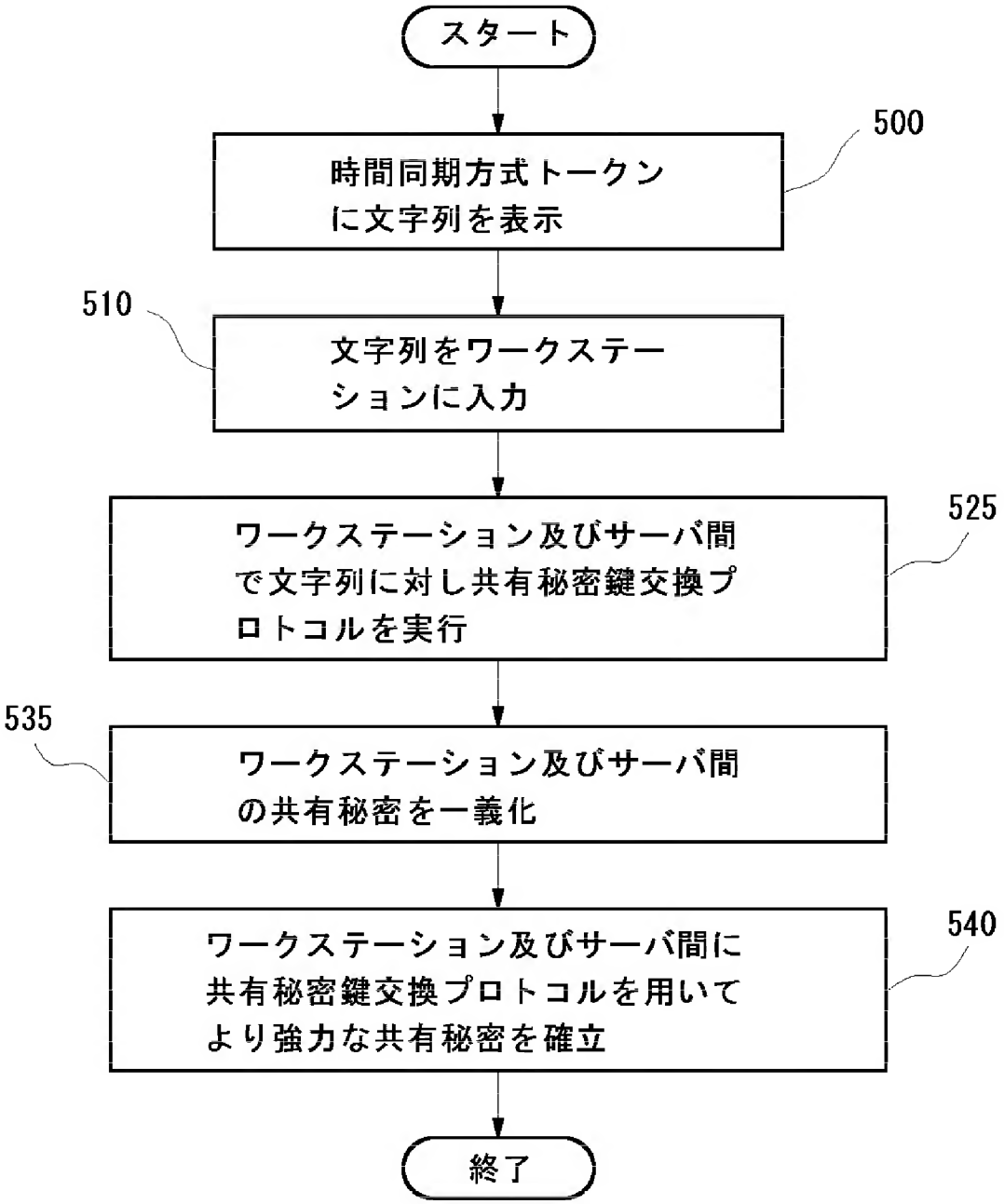

スタート
500
時間同期方式トークンに文字列を表示
510
文字列をワークステーションに入力
525
ワークステーション及びサーバ間で文字列に対し共有秘密鍵交換プロトコルを実行
535
ワークステーション及びサーバ間の共有秘密を一義化
540
ワークステーション及びサーバ間に共有秘密鍵交換プロトコルを用いてより強力な共有秘密を確立
終了

FIG. 5c

【図６】

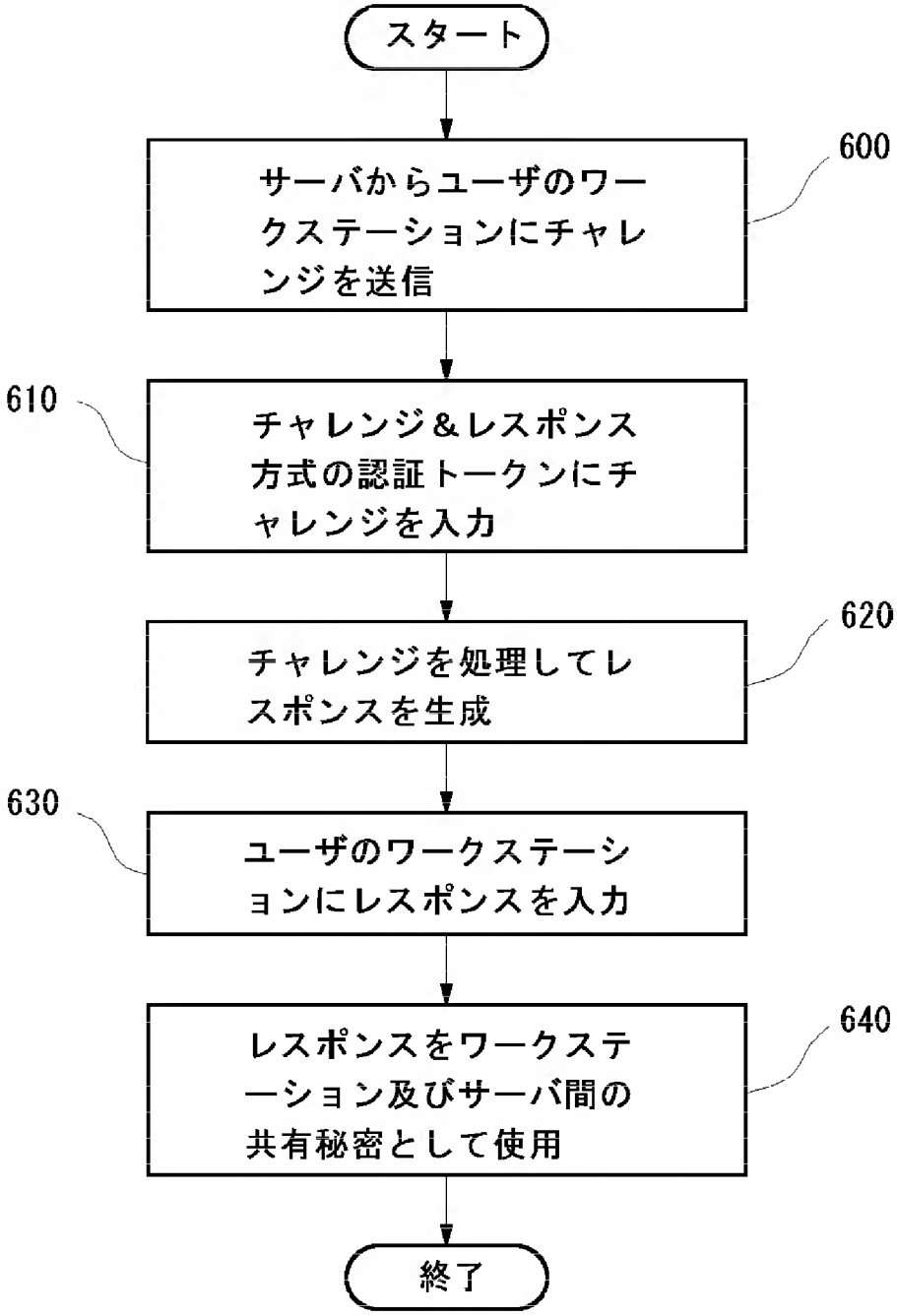

スタート
サーバからユーザのワークステーションにチャレンジを送信
600
610
チャレンジ＆レスポンス方式の認証トークンにチャレンジを入力
チャレンジを処理してレスポンスを生成
620
630
ユーザのワークステーションにレスポンスを入力
レスポンスをワークステーション及びサーバ間の共有秘密として使用
640
終了

FIG. 6

【図７】

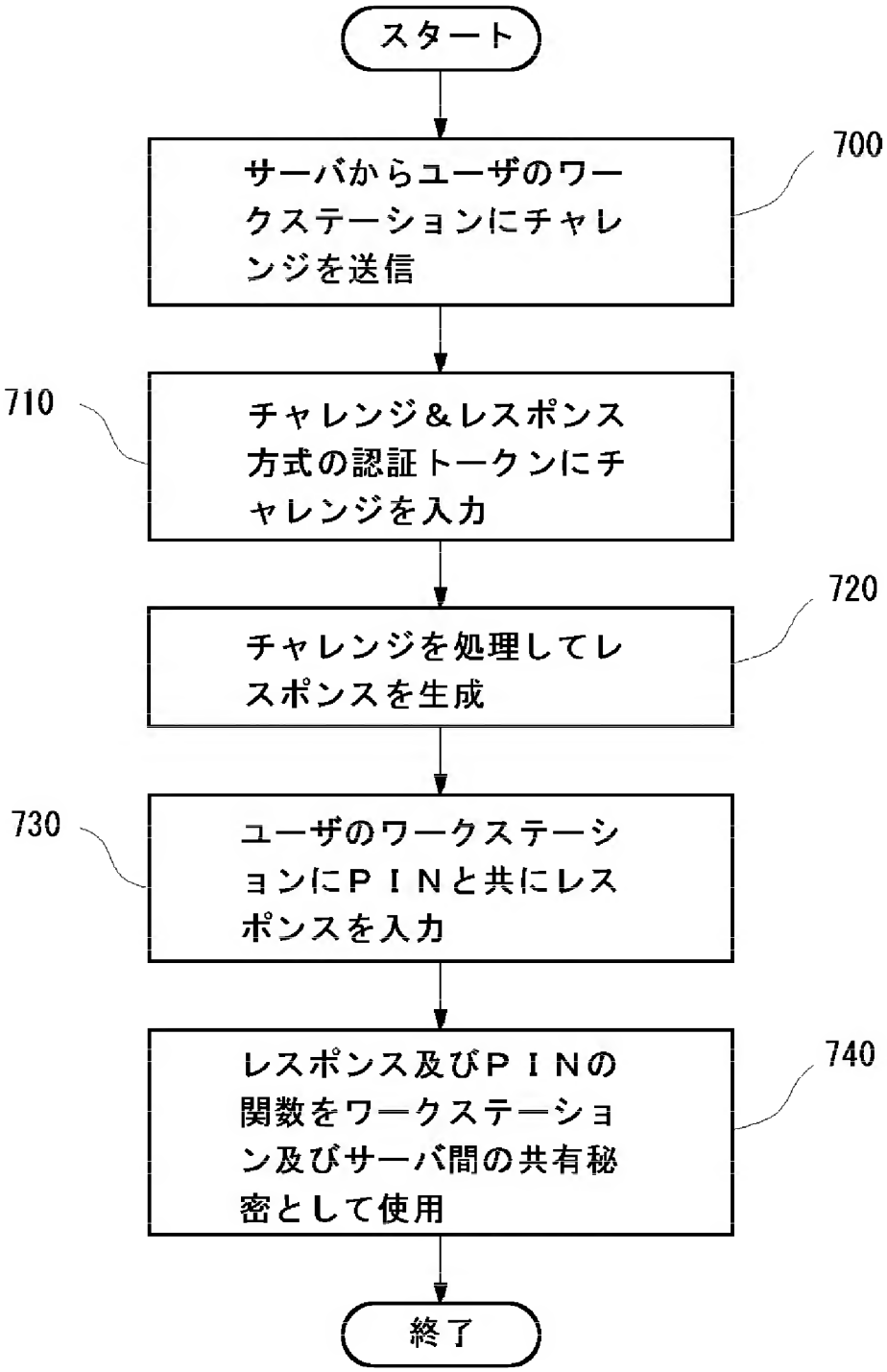

スタート
サーバからユーザのワークステーションにチャレンジを送信
700
チャレンジ＆レスポンス方式の認証トークンにチャレンジを入力
710
チャレンジを処理してレスポンスを生成
720
ユーザのワークステーションにＰＩＮと共にレスポンスを入力
730
レスポンス及びＰＩＮの関数をワークステーション及びサーバ間の共有秘密として使用
740
終了

FIG. 7

【図８】

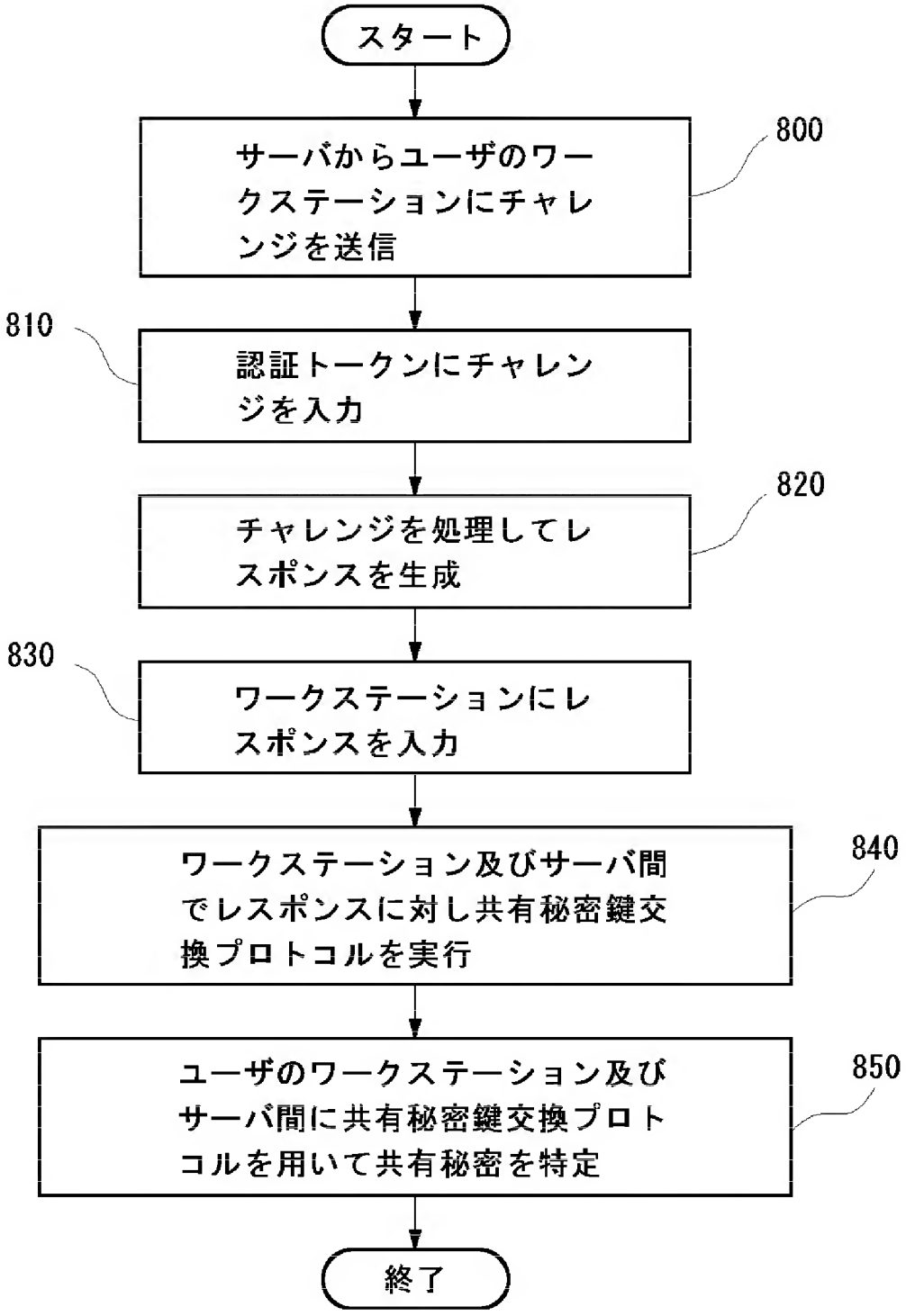

スタート
サーバからユーザのワークステーションにチャレンジを送信
800
認証トークンにチャレンジを入力
810
チャレンジを処理してレスポンスを生成
820
ワークステーションにレスポンスを入力
830
ワークステーション及びサーバ間でレスポンスに対し共有秘密鍵交換プロトコルを実行
840
ユーザのワークステーション及びサーバ間に共有秘密鍵交換プロトコルを用いて共有秘密を特定
850
終了

FIG. 8

【図９ａ】

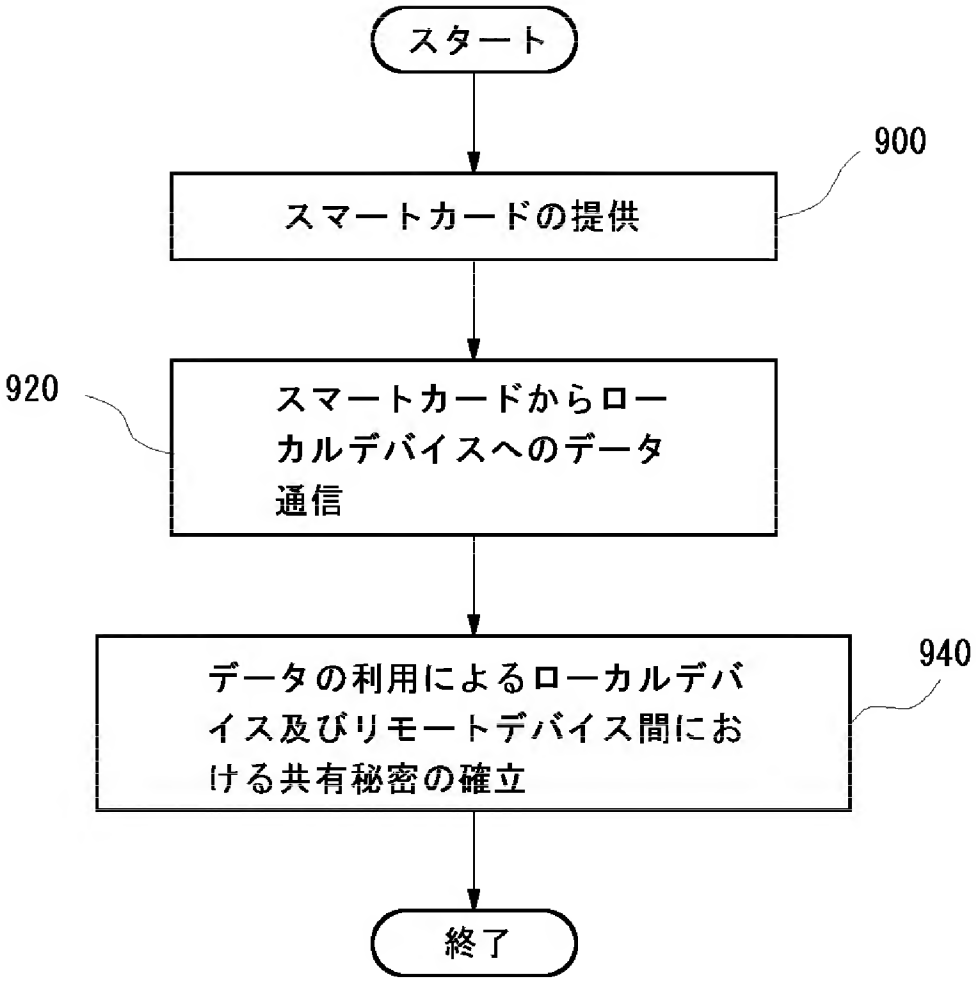

スタート
900
スマートカードの提供
920
スマートカードからローカルデバイスへのデータ通信
940
データの利用によるローカルデバイス及びリモートデバイス間における共有秘密の確立
終了

FIG. 9a

【図９ｂ】

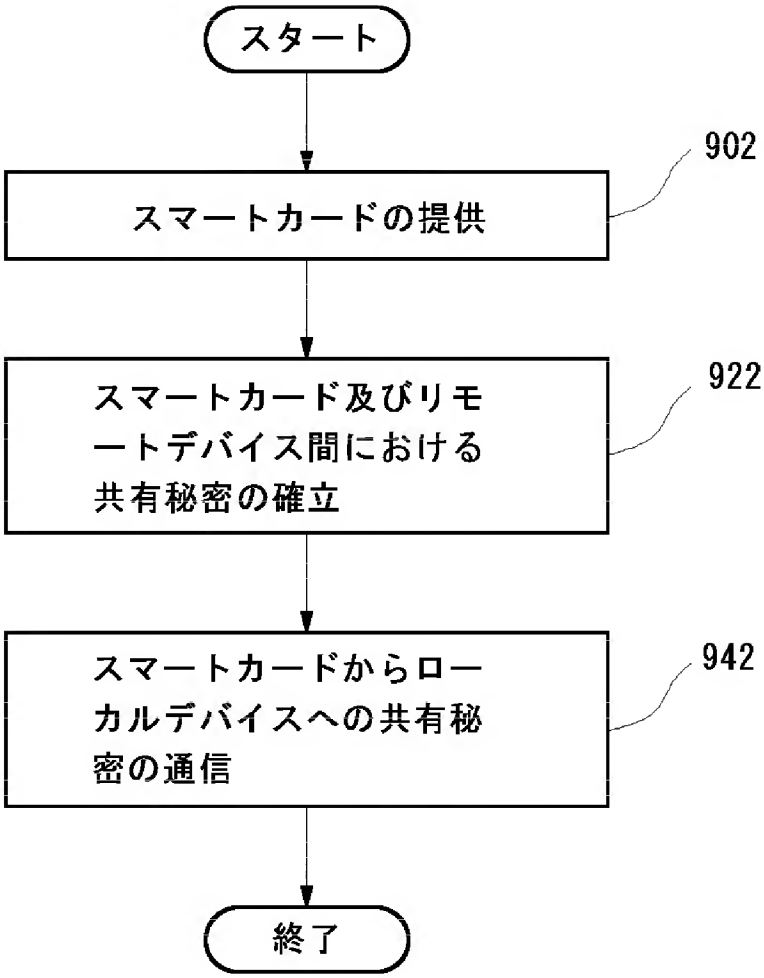

スタート
902
スマートカードの提供
922
スマートカード及びリモートデバイス間における共有秘密の確立
942
スマートカードからローカルデバイスへの共有秘密の通信
終了

FIG. 9b

【図９ｃ】

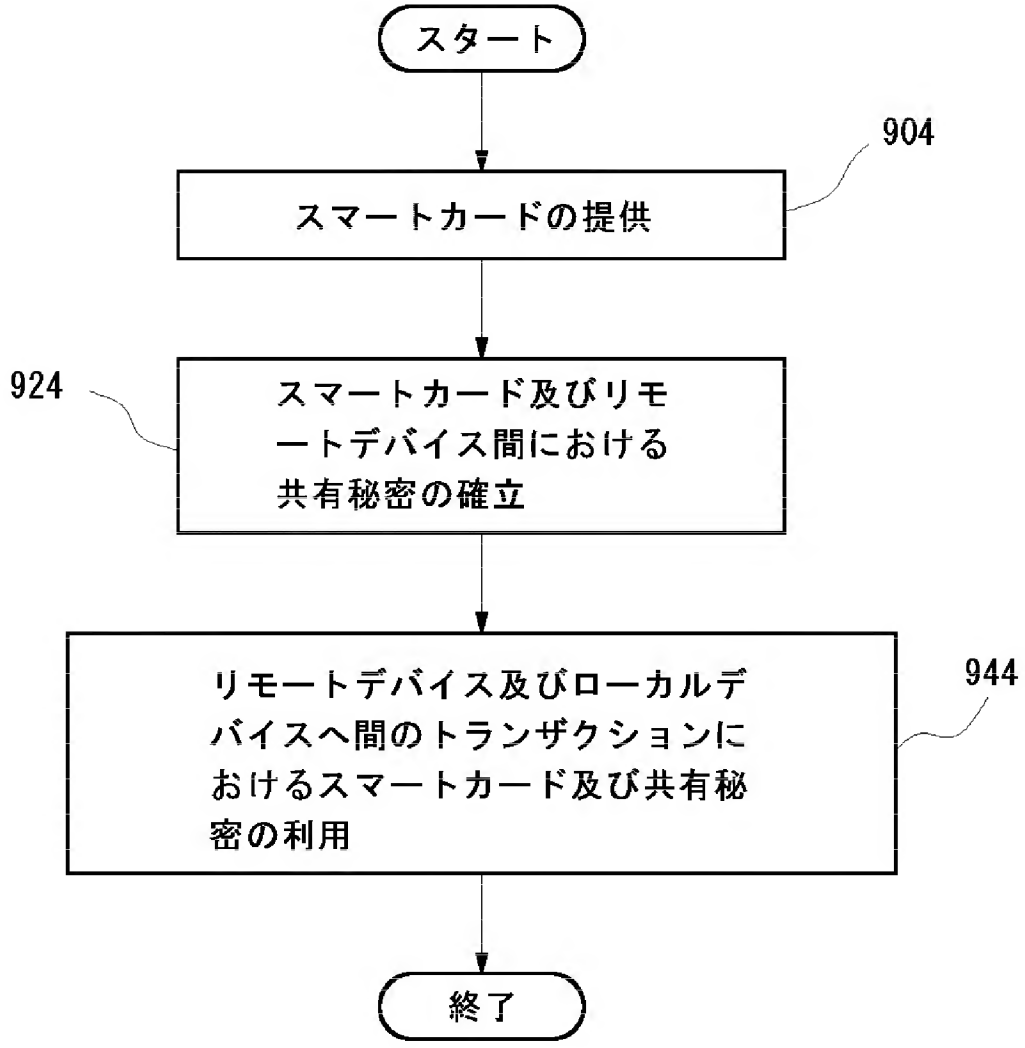

スタート
904
スマートカードの提供
924
スマートカード及びリモートデバイス間における共有秘密の確立
944
リモートデバイス及びローカルデバイスへ間のトランザクションにおけるスマートカード及び共有秘密の利用
終了

FIG. 9c

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/17232

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 602 918 A (CHEN JAMES F ET AL) 11 February 1997 (1997-02-11)	1,2,6,8, 9,18-23, 25-27, 29-31, 34-36, 47, 49-51, 58, 60-62, 64,66, 68-70,72
A	abstract column 2, line 36 - line 62 claim 1 figures 1,2,3A	11-17, 37,52

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 November 1999	18/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/17232

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 491 752 A (KAUFMAN CHARLES W ET AL) 13 February 1996 (1996-02-13) abstract column 5, line 48 - line 64 column 6, line 48 -column 7, line 47 column 8, line 24 - line 46 claim 1 figures 5-7	1-5,7,9, 11,13, 14,18, 19,25, 27,34, 35, 37-42,46
A	EP 0 566 811 A (IBM) 27 October 1993 (1993-10-27) abstract column 6, line 40 -column 7, line 47 column 8, line 7 - line 47 claim 1 figures 2,3	1-12, 25-37, 52-58, 66-73
P,X	US 5 892 902 A (CLARK PAUL C) 6 April 1999 (1999-04-06)	1,2,8,9, 11,18, 19, 25-36, 52-54, 56, 58-62, 64, 66-70,72
A	abstract column 2, line 5 - line 47 column 3, line 49 - line 62 column 4, line 13 - line 23 column 4, line 42 - line 44 claim 1 figures 2-5,7	20,37,47

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 99/17232

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5602918 A	11-02-1997	CA 2241052 A	03-07-1997
		EP 0870382 A	14-10-1998
		WO 9723972 A	03-07-1997
US 5491752 A	13-02-1996	US 5373559 A	13-12-1994
EP 0566811 A	27-10-1993	US 5347580 A	13-09-1994
US 5892902 A	06-04-1999	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国　　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者　ハンナ　ステファン　アール
アメリカ合衆国、01730　マサチューセッツ州、ベッドフォード、ビバリー　ロード　3

Fターム(参考)　5B058 CA27 KA02 KA04 KA08 KA31 KA35
5J104 AA04 AA07 KA02 KA03 KA06 NA02 NA03 NA11 NA12 NA35 NA40
5K030 GA15 HC01 KA01 KA06

【要約の続き】